Installation Procedures



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 |
| 04/17/2014 | Micah LaNasa | 1.0 | Initial draft for review |
|  |  |  |  |
|  |  |  |  |

Reviewers

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

Table of Contents

[1 Introduction 6](#_Toc390942691)

[2 Prerequisites 6](#_Toc390942692)

[3 Activating Azure RMS 11](#_Toc390942693)

[4 Create Custom Rights Policy Templates 12](#_Toc390942694)

[5 Install and Configure the RMS Connector 13](#_Toc390942695)

[6 Enabling Information Rights Management Functionality in Exchange 2010/2013 16](#_Toc390942696)

[7 Enabling Information Rights Management Functionality in Exchange Online 20](#_Toc390942697)

[8 Enabling Information Rights Management Functionality in SharePoint 2010/2013 23](#_Toc390942698)

[9 Enabling Information Rights Management Functionality in SharePoint Online 25](#_Toc390942699)

[10 Enabling Information Rights Management Functionality in Windows Server 2012 R2/Windows Server 2012 FCI 26](#_Toc390942700)

**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

This document is designed to give detailed information on how to deploy the solution components into production. The intended audience is the project’s deployment team.

This guide walks through the tasks involved in installing specific components of the infrastructure. The end to end process to deploy the Azure Rights Management Services (RMS) infrastructure at Customer Name is detailed in the Solution Deployment Plan document. That document calls the processes in this document as appropriate. This document can also be used to extend the pilot infrastructure after it has been deployed.

1. Prerequisites

Before activating Azure RMS, all prerequisites must be in place. A full discussion of each of these prerequisites is beyond the scope of this offering. Where appropriate, this guide links to additional supporting information. The following sections detail these prerequisites.

**Windows Azure tenant**: you must have already signed up for a Windows Azure tenant and have access to the credentials of an account with Global Administrator permissions in Office 365. For more information about Windows Azure Active Directory tenants, see the [Azure Active Directory tenant](http://technet.microsoft.com/en-us/library/dn655136.aspx#BKMK_AzureADTenant) TechNet article (<http://technet.microsoft.com/en-us/library/dn655136.aspx#BKMK_AzureADTenant>)

**Subscription to Azure RMS**: you must have already purchased a subscription to Azure RMS, either as a standalone service, or as part of a suite such as Office 365 or the Enterprise Mobility Suite. For more information about how to purchase a subscription to Azure RMS, see the [Cloud subscriptions that support Azure RMS](http://technet.microsoft.com/en-us/library/dn655136.aspx#BKMK_SupportedSubscriptions) TechNet article (<http://technet.microsoft.com/en-us/library/dn655136.aspx#BKMK_SupportedSubscriptions>).

**User/group accounts synchronized with Azure Active Directory**: you must have already synchronized user and group accounts from the on-premises Active Directory to the Azure Active Directory tenant. You can use the following tools to synchronize these accounts:

* **Directory Synchronization Tool**: The Directory Synchronization Tool is an on-premises application that periodically synchronizes user accounts to Azure Active Directory. Optionally, this tool can also synchronize users’ password hash, enabling them to authenticate to Azure Active Directory. Note that the Directory Synchronization Tool only supports a single Active Directory forest and user accounts must be coming from on-premises Active Directory.
* **Azure Active Directory Sync**: The Azure Active Directory Sync tool is the next generation version of the Directory Synchronization Tool. It also provides the ability to synchronize user accounts and passwords to Azure Active Directory. Unlike the Directory Synchronization Tool, the Azure Active Directory Sync tool supports multiple Active Directory forests synchronizing to a single Windows Azure tenant. It also supports additional account repositories, beyond Active Directory.
* **Microsoft Identity Manager**: Complex identity configurations may require the use of Microsoft Identity Manager, formerly Forefront Identity Manager (FIM). Microsoft Identity Manager is able to synchronize user accounts to Azure Active Directory in complex architectures. In some cases, Microsoft Identity Manager or Forefront Identity Manager may already be deployed onsite.

For more information about how to synchronize users to the cloud with Azure Active Directory, see the [Directory integration](http://technet.microsoft.com/en-us/library/jj573653.aspx) TechNet article (<http://technet.microsoft.com/en-us/library/jj573653.aspx>).

**(Optional) Active Directory Federation Services (AD FS)**: AD FS can be used to provide users with a single sign-on experience as they authenticate to Azure RMS and other cloud services integrated with Azure Active Directory. Also, in such a scenario, user password information remains on-premises. Authentication to Azure Active Directory is always routed to the on-premises Active Directory. For more information about how to deploy AD FS for use with Azure Active Directory, see the [Directory Sync with Single Sign-on Scenario](http://technet.microsoft.com/en-us/library/dn441213.aspx) TechNet article (<http://technet.microsoft.com/en-us/library/dn441213.aspx>).

**(Optional) Web Application Proxy (WAP)**: The Web Application Proxy is a role service within the Remote Access server role that can be used to configure AD FS for extranet access. This prevents you from exposing your AD FS servers directly to the Internet. For more information about how to deploy WAP for use with AD FS in Azure Active Directory see the [Configure extranet access for AD FS on Windows Server 2012 R2](http://msdn.microsoft.com/en-us/library/azure/dn528859.aspx) MSDN article (<http://msdn.microsoft.com/en-us/library/azure/dn528859.aspx>).

1. Generating and Transferring the Azure RMS Tenant Key

*If your customer is not going to use the BYOK functionality, delete this section.*

The following steps are used to help generate and securely transfer a tenant key for your Azure RMS subscription. These steps assume that you have already implemented the necessary Thales Hardware Security Module hardware and software components and that you have a basic operational knowledge of Thales HSMs. For more information about Thales HSMs, see [Thales Hardware Security Modules](https://www.thales-esecurity.com/msrms/buy) (<https://www.thales-esecurity.com/msrms/buy>).

*Your customer can decide to generate the key and transfer it in person at Microsoft datacenter or to transfer it via the Internet. Delete the appropriate section*

*In Person*

1. Create the Security World
   1. Log on to a computer that has the Thales nCipher support software installed on it. Confirm that the computer has connectivity to the Thales HSM.
   2. Open a command prompt window.
   3. In the command prompt window navigate to C:\Program Files (x86)\nCipher\nfast\bin
   4. Type the following command and press Enter: new-world.exe --initialize --km-type=rijndael --module=1 –acs-quorum=*k*/*n* where k is your quorum and n is the total number of Administrator cards.
   5. Enter the Administrator cards as required and, optionally, provide a password for each card.
   6. Back up the Security World according to the specifications provided by Thales.
2. Create the tenant key
   1. On the computer you used in step 1, open a command prompt window.
   2. In the command prompt window navigate to C:\Program Files (x86)\nCipher\nfast\bin
   3. Type the following command and press Enter: generatekey --generate simple type=RSA size=2048 protect=module ident=*name* plainname=*name* nvram=no pubexp= where name is any string value that helps you identify the key. We recommend using all lower case characters.
   4. Type the following command and press Enter: cngimport --import –M --key=*name* --appname=simple *name* where name is the name specified in step b.
   5. This command will generate a key file located in the %NFAST\_KMDATA%\local folder. This is the file that contains the encrypted key.
   6. Back up the key according to the specifications provided by Thales.
3. Transfer the tenant key to the Azure RMS Security World
   1. Contact Microsoft Customer Support Services (CSS) to schedule a key transfer appointment.
   2. Bring your key file generated in the step above on a USB device, a copy of your Security World file, and a quorum of Administrator Cards.
   3. Microsoft personnel will walk you through the process of securely transferring the tenant key to the Microsoft datacenters.

*Over the Internet*

This process requires a client computer with Internet access and a second client computer disconnected from the network and from the Internet.

1. Prepare the online client computer
   1. Log on to a computer running Windows Vista or later or Windows Server 2008 or later with Windows PowerShell 2.0 or later.
   2. Download the Microsoft Online Services Sign-In Assistant from the [Microsoft Download Center](http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=28177) (<http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=28177>).
   3. Navigate to the folder that contains the downloaded file. Double click the source file to open the Microsoft Online Services Sign-in Assistant Setup installation wizard.
   4. On the Welcome screen, click Next.
   5. On the Licensing screen, select the I accept the terms in the License Agreement and Privacy Statement option and click Install.
   6. Verify that the installation was successful and click Finish.
   7. Download the Azure AD Rights Management Administration Tool from the [Microsoft Download Center](http://www.microsoft.com/en-us/download/details.aspx?id=30339) (<http://www.microsoft.com/en-us/download/details.aspx?id=30339>).
   8. Navigate to the folder that contains the downloaded file. Double click the source file to open the Windows Azure AD Rights Management Administration Setup Wizard.
   9. On the Welcome screen click Next.
   10. On the Licensing screen, select the I accept the terms in the License Agreement option and click Next.
   11. On the Ready to install screen, click Install.
   12. Verify that the installation was successful and click Finish.
   13. Open Windows PowerShell with elevated permissions.
   14. Type the following command in Windows PowerShell and press Enter: Import-module aadrm
   15. Type the following command in Windows PowerShell and press Enter: Connect-AadrmService
   16. Enter the user name and password of an account with Office 365 global administrator credentials.
   17. Type the following command in Windows PowerShell and press Enter: Get-AadrmConfiguration
   18. Review the BPOSId in the first line. It should appear in the form of a GUID. This is your Azure Active Directory tenant ID. Copy the value and paste to a location you can reference later.
   19. Type the following command in Windows PowerShell and press Enter: Disconnect-AadrmService
   20. Close Windows PowerShell.
   21. Download the BYOK toolset that is specific for the geographic region from the [Microsoft Download Center](http://go.microsoft.com/fwlink/?LinkId=335781) (<http://go.microsoft.com/fwlink/?LinkId=335781>).
   22. Copy the toolset to a portable storage device that you can use to transfer the to the offline client computer.
2. Prepare the offline client computer
   1. Log on to an offline computer with the Thales nCipher support software installed. Ensure that the computer has connectivity to the Thales HSM. For more information about how to install the Thales software, visit the [Thales](https://www.thales-esecurity.com/msrms/cloud) website (<https://www.thales-esecurity.com/msrms/cloud>).
   2. Copy the BYOK toolset from the portable storage device referenced in step 1.
   3. Extract the files within the toolset to a folder of your choice.
   4. Navigate to that folder and double click the vcredist\_x64.exe file.
   5. Follow the instructions to install the Visual C++ runtime components for Visual Studio 2012.
3. Generate your tenant key
   1. Log on to the offline computer and open a command prompt window.
   2. In the command prompt window navigate to C:\Program Files (x86)\nCipher\nfast\bin
   3. Type the following command and press Enter: new-world.exe --initialize --km-type=rijndael --module=1 –acs-quorum=*k*/*n* where *k* is your quorum and *n* is the total number of Administrator cards.
   4. Enter the Administrator cards as required and, optionally, provide a password for each card.
   5. Back up the Security World according to the specifications provided by Thales.
   6. Type the following command and press Enter: generatekey --generate simple type=RSA size=2048 protect=module ident=*name* plainname=*name* nvram=no pubexp= where name is any string value that helps you identify the key. We recommend using all lower case characters.
   7. Type the following command and press Enter: cngimport --import –M --key=*name* --appname=simple *name* where name is the name specified in step b.
   8. This command will generate a key file located in the %NFAST\_KMDATA%\local folder. This is the file that contains the encrypted key.
   9. Back up the key according to the specifications provided by Thales.
4. Prepare a copy of the tenant key
   1. Log on to the offline computer and open a command prompt window.
   2. Type one of the following commands and press Enter. Note that you must replace *name* with the same value specified above:
      1. North America: KeyTransferRemote.exe -ModifyAcls -KeyAppName simple -KeyIdentifier *name* -ExchangeKeyPackage BYOK-KEK-pkg-NA-1 -NewSecurityWorldPackage BYOK-SecurityWorld-pkg-NA-1
      2. Europe: KeyTransferRemote.exe -ModifyAcls -KeyAppName simple -KeyIdentifier *name* -ExchangeKeyPackage BYOK-KEK-pkg-EU-1 -NewSecurityWorldPackage BYOK-SecurityWorld-pkg-EU-1
      3. Asia: KeyTransferRemote.exe -ModifyAcls -KeyAppName simple -KeyIdentifier *name* -ExchangeKeyPackage BYOK-KEK-pkg-AP-1 -NewSecurityWorldPackage BYOK-SecurityWorld-pkg-AP-1
   3. Verify that you receive a message that states that the result was successful.
   4. To encrypt your key using Microsoft Key Exchange Key, type one of the following commands and press Enter. Note that you should replace *FriendlyName* with a name to help you identify your key. This is a new value. Also, replace *GUID* with the Azure Active Directory tenant ID you copied in step 1 and replace *name* with the identifier that you used in when you generated the tenant key:
      1. North America: KeyTransferRemote.exe -Package -KeyIdentifier *name* -ExchangeKeyPackage BYOK-KEK-pkg-NA-1 -NewSecurityWorldPackage BYOK-SecurityWorld-pkg-NA-1 -TenantBposId *GUID* -KeyFriendlyName *FriendlyName*
      2. Europe: KeyTransferRemote.exe -Package -KeyIdentifier *name* -ExchangeKeyPackage BYOK-KEK-pkg-EU-1 -NewSecurityWorldPackage BYOK-SecurityWorld-pkg-EU-1 -TenantBposId *GUID* -KeyFriendlyName *FriendlyName*
      3. Asia: KeyTransferRemote.exe -Package -KeyIdentifier *name* -ExchangeKeyPackage BYOK-KEK-pkg-AP-1 -NewSecurityWorldPackage BYOK-SecurityWorld-pkg-AP-1 -TenantBposId *GUID* -KeyFriendlyName *FriendlyName*
   5. Verify that you receive a message that indicates that the operation was successful.
   6. Verify that the command has created a new file named TransferPackage-*FriendlyName.*byok.
   7. Copy the BYOK file to a portable storage device and transfer it to the online computer.
5. Transfer the key to Azure RMS
   1. On the online computer, open Windows PowerShell.
   2. Type the following command and press Enter: Connect-AadrmsService
   3. Type the following command and press Enter: Get-AadrmKeys
   4. Type the following command and press Enter: Add-AadrmKey –KeyFile FileLocation –Verbose
   5. Confirm that you wish to upload the key.
   6. Verify that you receive a message that indicates that the operation was successful.
   7. Type the following command and press Enter: Get-AadrmKeys. Verify that the new key has been uploaded.
6. Activating Azure RMS

By default, Azure RMS is turned off. When <<Customer Name>> activates Azure RMS, the feature will be turned on for all rights-enabled services and applications. Azure RMS must be activated before end users can create and consume protected content within Office, the RMS App, Exchange, SharePoint, and FCI/Work Folders. The following steps walk through the process to activate Azure RMS. The steps assume a tenant in Windows Azure and a subscription to the Azure RMS service.

1. Activate Azure RMS
   1. Log in to Office 365 with an account with Global Administrator permissions or equivalent.
   2. Click Service Settings.
   3. In the Service Settings page, click Rights Management.
   4. In the Protect your information section, click Manage.
   5. In the Rights management section, click Activate.
   6. Click Activate in the popup box.
   7. Verify that the message Rights management is activated appears in the Rights management section.

1. Create Custom Rights Policy Templates

Azure RMS includes two built-in rights policy templates as follows:

* Company Confidential:
* Company Confidential Read Only:

However, you may want to create custom rights policy templates to support additional use cases. For example, you can use a custom rights policy template to grant rights to a subset of users in the organization, rather than all users in the tenant. You can also configure custom permissions or additional permission options. The following steps describe how to create and publish custom rights policy templates.

1. Create a custom rights policy template
   1. Access the Get started with Rights Management quick start page from the Office 365 admin center or from the Azure Management Portal.
   2. Click Create a new rights policy template to start the Rights Policy Template wizard.
   3. In the Add a new rights policy template window, choose the appropriate language for the rights policy template and enter a name and description for the template. You can assign name and description to a template in different languages, and to assure proper usage and non-deniability, you should do so for all the different languages in use in your organization. Click the Complete icon.
   4. Click Manage your rights policy templates and select the newly created template.
   5. Under Configure rights for users and groups click Get started.
   6. Click Get started now.
   7. In the Select users and groups window, locate and click the appropriate users or groups. Click the Next icon to continue.
   8. Select the appropriate permission level and click the Complete icon.
   9. Click Add and repeat the previous two steps to add additional users and groups with different permissions
   10. Click the Configure tab.
   11. If desired, add the template name and description in additional languages.
   12. If desired, configure content expiration by date or number of days.
   13. If desired, configure offline access.
   14. Repeat these steps to create additional rights policy templates.
2. Publish a custom rights policy template.
   1. Access the Get started with Rights Management quick start page from the Office 365 admin center or from the Azure Management Portal.
   2. Click Templates to display a list of the available rights policy templates.
   3. Click the rights policy template that you would like to publish.
   4. Click Configure.
   5. In the General section select Publish.
   6. Click Save.
   7. Repeat these steps to publish additional rights policy templates.
3. Configure RMS Administration

Most administrative tasks in Azure RMS are performed using the Windows PowerShell module for Azure Rights Management. The following steps detail how to install the module and begin administering Azure RMS.

1. Install the Microsoft Online Services Sign-in Assistant
   1. Log on to a computer running Windows Vista or later or Windows Server 2008 or later with Windows PowerShell 2.0 or later.
   2. Download the Microsoft Online Services Sign-In Assistant from the [Microsoft Download Center](http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=28177) (<http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=28177>).
   3. Navigate to the folder that contains the downloaded file. Double click the source file to open the Microsoft Online Services Sign-in Assistant Setup installation wizard.
   4. On the Welcome screen, click Next.
   5. On the Licensing screen, select the I accept the terms in the License Agreement and Privacy Statement option and click Install.
   6. Verify that the installation was successful and click Finish.
2. Install the Rights Management administration module
   1. On the computer you used in step 1, download the Azure AD Rights Management Administration Tool from the [Microsoft Download Center](http://www.microsoft.com/en-us/download/details.aspx?id=30339) (<http://www.microsoft.com/en-us/download/details.aspx?id=30339>).
   2. Navigate to the folder that contains the downloaded file. Double click the source file to open the Windows Azure AD Rights Management Administration Setup Wizard.
   3. On the Welcome screen click Next.
   4. On the Licensing screen, select the I accept the terms in the License Agreement option and click Next.
   5. On the Ready to install screen, click Install.
   6. Verify that the installation was successful and click Finish.
3. Administer Azure RMS
   1. On the computer you used in steps 1 and 2, open Windows PowerShell with elevated permissions.
   2. Type the following command in Windows PowerShell and press Enter: Import-Module AADRM
   3. Type the following command in Windows PowerShell and press Enter: Connect-AadrmService –Verbose
   4. Enter the user name and password of an account with Office 365 global administrator permissions.
   5. You can now begin administering Azure RMS.
4. Configure Logging

Azure RMS logs every request that it makes for the organization, which includes requests from end users, such as for use licenses or certificates, actions performed by RMS administrators in the organizations, and actions performed by Microsoft operators to support the RMS deployment. The following steps demonstrate how to enable logging in Azure RMS. This steps assume you have already completed the steps in the previous sections and that you have a subscription to Windows Azure and sufficient storage in Azure for the RMS logs. Note that Azure RMS logging will require on-going maintenance. For more information about how to manage your Azure RMS logs, review the Azure\_RMS\_06\_Stabilize\_DELIVERY\_Operations-Guide document.

1. Create a storage account in Windows Azure
   1. Log in to the [Azure Management Portal](https://manage.windowsazure.com/) (<https://manage.windowsazure.com/>) with an Azure account.
   2. In the left pane, click Storage.
   3. Click Create a storage account and enter a name for the new storage account.
   4. Select the particular geographic region that most closely matches yours.
   5. Click OK. Verify that the new storage name has a status of Online before continuing.
   6. Click Manage Access Keys.
   7. Find the primary access key, copy it, and paste it to a location you can access it in the next step.
2. Enable Azure RMS Logging
   1. Open Windows PowerShell with elevated permissions.
   2. Type the following command in Windows PowerShell and press Enter: Connect-AadrmService
   3. If prompted, provide a user name and password for an account with Azure RMS Administrator permissions or equivalent.
   4. Type the following command in Windows PowerShell and press Enter. Note that you must replace *KeyValue* with the primary access key you copied in the previous step: $accesskey = convertto-securestring -asplaintext -force –string *KeyValue*
   5. Type the following command in Windows PowerShell and press Enter. Note that you must replace *AccountName* with the name of the Storage Account, as configured in the previous step: Set-AadrmUsageLogStorageAccount -AccessKey $accesskey -StorageAccount *AccountName*
   6. Type the following command in Windows PowerShell and press Enter: Enable-AadrmUsageLogFeature
   7. Verify that you receive a message that the log feature was successfully enabled.
3. Install and Configure the RMS Connector

The RMS Connector is an on-premises tool that enables on-premises server-side applications such as Exchange Server, SharePoint Server and File Classification Infrastructure to utilized built-in IRM integration features with Azure RMS.

To enable on-premises server-side applications to use Azure RMS, follow these steps:

1. Create the associated DNS record
   1. Log on to a DNS server with a domain account with domain admin permissions or equivalent.
   2. Open the DNS console.
   3. Expand Forward Lookup Zones and expand the domain. Right click in the details pane and select New Host (A or AAAA).
   4. In the Name field, enter an appropriate DNS name, for example connector.
   5. In the IP Address field, enter the IP address of the RMS Connector server or load balancing technology.
   6. Verify that the Create associated pointer (PTR) record option is selected and click Add Host.
   7. Close the DNS console.
2. Install the RMS Connector
   1. Log on to a server in the cluster with a domain account with local administrative permissions or equivalent.
   2. Download the source files for the RMS Connector from the [Microsoft Download Center](http://www.microsoft.com/en-us/download/details.aspx?id=40839) (<http://www.microsoft.com/en-us/download/details.aspx?id=40839>).
   3. Navigate to the location of the source files.
   4. Select and right-click the RMSConnectorSetup.exe file and select Run as administrator.
   5. On the Welcome page, select Install Microsoft Rights Management connector on the computer and click Next.
   6. On the License page, review the licensing terms, accept the licensing terms, and click Next.
   7. On the Credential page, enter the username and the password of an Azure tenant administrator. Click Next.
   8. On the Confirmation page, click Install.
   9. Verify that the tool installed correctly and click Finish.
3. Authorize Server-side Applications to use the Connector
   1. Log on to the RMS Connector server.
   2. Open the Microsoft RMS Connector administration Tool.
   3. If necessary, provide the user name and password of an Azure RMS Administrator.
   4. On the Servers allowed to utilize the connector page, click Add.
   5. On the Allow a server to utilize the connector window, click the Role drop down and select the appropriate role.
   6. Click Browse, enter the appropriate computer, group, or service account name, click Check Names, and click OK.
      1. For Exchange servers, specify a security group that contains all of the computer accounts of the Exchange servers. Typically, the All Exchange Servers default group can be used.
      2. For SharePoint servers, add a security group that contains all of the computer accounts of the SharePoint servers and/or the service account that runs the SharePoint Central Administration service and the account that is configured for the SharePoint App Pool. This selection will depend on how your SharePoint architecture is configured.
      3. For FCI servers, add a security group that contains all of the computer accounts of the servers running FCI.
   7. Click OK.
   8. Repeat steps d through g to add additional computers, groups, or service names.
   9. Click Close to close the Microsoft Rights Management Connector administration tool.
4. Configure High Availability
   1. Install the RMS connector on one or more additional servers using the steps presented in step 2.
   2. Add the relevant computer and service accounts to the newly configured servers using the steps presented in step 3.
   3. Configure load balancing for the IP address created in step 1 and direct the traffic to the connector servers. Any IP-based load balancer can be used for this purpose, including the Network Load Balancing feature in Windows Server. Use the following settings to configure the NLB cluster:
      1. Port: 80 (for HTTP) or 443 (for HTTPS)
      2. Affinity: None
      3. Distribution Method: Equal
5. Configure the RMS Connector to use HTTPS (optional)
   1. Create or procure a server authentication certificate that contains the DNS name configured in step 1. Verify that the certificate chains to a root CA that the Exchange/SharePoint/FCI servers trust.
   2. Install this certificate on each of the RMS Connector servers.
   3. Bind the certificate to the Default Web Site in the IIS Console.
6. Configure the RMS Connector for a web proxy server (optional)
   1. Log on to the RMS Connector server with local administrative permissions or equivalent.
   2. Click Start, type regedit in the Search field, and click Registry Editor to open the Registry Editor.
   3. Navigate to the following registry path: ****HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\AADRM\Connector****
   4. **Add the string value of **ProxyAddress** and set the data value for this value to be **http://<***ProxyDomainorIPAddress***>:<***ProxyPort*>**
   5. **Close the Registry Editor and restart the server.**
   6. **Repeat these steps for each server running the RMS Connector.**
7. Enabling Information Rights Management Functionality in Exchange 2010/2013

*If your customer is not going to use IRM functionality in Exchange 2010/2013, delete this section.*

The following steps are used to enable basic Information Rights Management (IRM) integration for Microsoft Exchange Server 2010/2013. The corresponding Exchange Server roles (Hub Transport servers for Transport Protection, Journal Decryption, Prelicensing and Transport Decryption, and CAS for OWA IRM and IRM Search) must be installed in a server with the Rights Management Services Client installed and configured like a normal client computer.

1. Retrieve the Azure RMS URL for the tenant.
   1. Log on to a computer with the Azure AD Rights Management Administration Tool as a local administrator or equivalent.
   2. From the Start screen, enter **PowerShell** in the Search field.
   3. Right click the **PowerShell** icon and select **Run as administrator**.
   4. Type the following command and press **Enter**: **Import-module aadrm**
   5. Type the following command and press **Enter**: **Connect-aadrmService**
   6. Enter the user name and password of an Azure Active Directory Administrator account and press **Enter**.
   7. Type the following command and press **Enter**: **Get-AadrmConfiguration**
   8. The Microsoft RMS URL will be returned in a format that resembles the following example. Copy the URL for use when changing registry keys on the Exchange servers: **https://5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com**
   9. Close Windows PowerShell and log off of the computer.
2. Modify the registry information to point to the RMS Connector
   1. Log on to the Exchange server with an account with local administrative permissions or equivalent.
   2. From the Start menu, type **Regedit** in the Search Field and click **Registry Editor** to open the Registry Editor.
   3. Navigate to the following registry key: **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\MSDRM\ServiceLocation\Activiation**. If any keys within the path do not exist, create them.
   4. Create a new Reg\_SZ in the Activation node, leaving the value as **Default**.
   5. Double click the new Reg\_SZ and enter the Azure RMS tenant URL you copied in step one in the Data field.
   6. Click **OK**.
   7. Navigate to the following registry key: **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\MSDRM\ServiceLocation\EnterprisePublishing**. If any keys within the path do not exist, create them.
   8. Create a new Reg\_SZ in the EnterprisePublishing node leaving the value as **Default**.
   9. Double click the new Reg\_SZ and enter the Azure RMS tenant URL you copied in step one in the Data field.
   10. Click **OK**.
   11. Navigate to the following registry key: **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\ExchangeServer**\v15 or v14\**IRM\CertificationServerRedirection**. If any keys within the path do not exist, create them.
   12. Create a new Reg\_SZ in the CertificationServerRedirection node with a value of the Azure RMS tenant URL you copied in step one.
   13. Double click the new Reg\_SZ and enter the RMS Connector URL in the Data field.
   14. Click **OK**.
   15. Navigate to the following registry key: H**KEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\ExchangeServer\**v15 or v14\**IRM\LicenseServerRedirection**. If any keys within the path do not exist, create them.
   16. Create a new Reg\_SZ in the LicenseServerRedirection node with a value of the Azure RMS tenant URL you copied in step one.
   17. Double click the new Reg\_SZ and enter the RMS Connector URL in the Data field.
   18. Click **OK**.
   19. Close the Registry Editor and log off of the server.
   20. Repeat these steps for each Exchange server that will use Azure RMS.
3. To enable OWA IRM and IRM Search support:
   1. Log on to the mail server as an Administrator.
   2. Open the **Exchange Management Shell** from the **Start Menu**.
   3. To enable IRM in OWA type the following command in the **Exchange Management Shell**:

Get-OWAMailboxPolicy

* 1. Look for the **IRMEnabled** parameter. If it is not set to **True**, run the following command:

Set-OWAMailboxPolicy –Identity Default -IRMEnabled $true

Set-IRMConfiguration -OWAEnabled $true

1. The first command enables or disables IRM for a specific mailbox; the second one enables it at the server level.
   1. To verify if indexing for search of protected content in OWA is enabled type the following command in the **Exchange Management Shell**:

Get-IRMConfiguration

* 1. Look for the **SearchEnabled** parameter. If it is not set to **True**, run the following command:

Set-IRMConfiguration -SearchEnabled $true

* 1. For this functionality to work, Internal Licensing must be enabled. Type the following command in the Exchange Management Shell:

Get-IRMConfiguration

* 1. Look for the **InternalLicensingEnabled** parameter. If it is not set to **True**, run the following command:

Set-IRMConfiguration –InternalLicensingEnabled $true

1. Create Transport Protection Rules
   1. Open the Exchange Admin Center.
   2. Click **mail flow** to open the rules tab.
   3. Click the plus icon and select **Apply rights protection to messages** to open the new rule editor.
   4. Enter a name in the Name field
   5. In the Apply this rule if drop down, select the appropriate condition that will trigger RMS protection, for example, you could select **The subject or body matches** to look for specific words or number patterns.
   6. Add the parameters of the condition. Continuing with the above example, you could add **Top Secret** to automatically protect any message with the phrase Top Secret in the subject or body of the message. Click **OK**.
   7. In the Do the following section, click **Select one** and select the appropriate rights policy template.
   8. If desired, add an exception or audit configuration.
   9. Click **Save**.
   10. Repeat these steps to add additional transport protection rules.
2. To enable Transport Decryption:
   1. Log on to the mail server as an Administrator.
   2. Open the **Exchange Management Shell** from the **Start Menu**.
   3. To enable Transport Decryption type the following command in the **Exchange Management Shell**:

Set-IRMConfiguration -TransportDecryptionSetting Mandatory

1. To enable Journal Decryption:
   1. Log on to the mail server as an Administrator.
   2. Open the **Exchange Management Shell** from the **Start Menu**.
   3. To enable Journal Decryption type the following command in the **Exchange Management Shell**:

Set-IRMConfiguration -JournalReportDecryptionEnabled $true

1. Integrate the Exchange Data Loss Prevention feature with RMS
   1. Open the Exchange Admin Center.
   2. Click **compliance management** and then click the **data loss prevention** tab.
   3. Click the plus icon and select **New DLP policy from template** to open the DLP policy from template wizard.
   4. Add a name and description.
   5. Select a template that matches the geographic region and vertical industry and click **Save**.
   6. Click the **mail flow** tab.
   7. Double click one of the rules that was created from the DLP policy above.
   8. Under the Do the following section, click the drop down, point to **Modify the message security** and **select Apply rights protection**.
   9. Select the appropriate rights policy template and click **OK**.
   10. Click **Save**.
   11. Repeat steps h through k to edit additional rules associated with the DLP policy.
   12. Repeat steps a through l to add additional DLP policies integrate with RMS.
2. Enabling Information Rights Management Functionality in Exchange Online

*If your customer is not going to use IRM functionality in Exchange Online, delete this section.*

The following steps are used to enable basic Information Rights Management (IRM) integration for Exchange Online.

Before you begin, identify the RMS Online key sharing URL that corresponds to your location:

|  |  |
| --- | --- |
| Location | RMS Key Sharing Location |
| North America | <https://sp-rms.na.aadrm.com/TenantManagement/ServicePartner.svc> |
| European Union | <https://sp-rms.eu.aadrm.com/TenantManagement/ServicePartner.svc> |
| Asia | <https://sp-rms.ap.aadrm.com/TenantManagement/ServicePartner.svc> |
| South America | <https://sp-rms.sa.aadrm.com/TenantManagement/ServicePartner.svc> |
| Office 365 for Government | <https://sp-rms.govus.aadrm.com/TenantManagement/ServicePartner.svc> |

1. Configure Exchange Online to use Azure RMS
   1. Log on to a computer with Windows PowerShell installed and access to the Internet
   2. From the Start menu, type PowerShell in the Search field, right click Windows PowerShell, and select Run as administrator to open Windows PowerShell.
   3. Type the following command and press **Enter**: **$LiveCred = Get-Credential**
   4. Enter the user name and password of an account with Office 365 global administrator permissions.
   5. Type the following command and press **Enter**:$Session = **New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri** [**https://ps.outlook.com/powershell/**](https://ps.outlook.com/powershell/) **-Credential $LiveCred -Authentication Basic –AllowRedirection**
   6. Type the following command and press **Enter**:**Import-PSSession $Session**
   7. Type the following command and press **Enter**: **Set-IRMConfiguration –RMSOnlineKeySharingLocation** *URL from above table* "
   8. Type the following command and press **Enter**: **Import-RMSTrustedPublishingDomain -RMSOnline -name "RMS Online”**
   9. Type the following command and press **Enter**: **Set-IRMConfiguration -InternalLicensingEnabled $true**
2. Enable Transport Decryption
   1. From a Windows PowerShell session connected to Exchange Online, type the following command and press **Enter**: **Set-IRMConfiguration –TransportDecryptionSetting Mandatory**
3. Enable Journal Decryption
   1. From a Windows PowerShell session connected to Exchange Online, type the following command and press **Enter**: **Set-IRMConfiguration –JournalReportDecryptionEnabled $true**
4. Create Transport Protection Rules
   1. Log on to Office 365 with an account with Office 365 Global Administrator permissions.
   2. From the Office 365 admin center, click the **Admin** drop down and select **Exchange**.
   3. Click **mail flow** to open the rules tab.
   4. Click the plus icon and select **Apply rights protection to messages** to open the new rule editor.
   5. Enter a name in the Name field
   6. In the Apply this rule if drop down, select the appropriate condition that will trigger RMS protection, for example, you could select **The subject or body matches** to look for specific words or number patterns.
   7. Add the parameters of the condition. Continuing with the above example, you could add **Top Secret** to automatically protect any message with the phrase Top Secret in the subject or body of the message. Click **OK**.
   8. In the Do the following section, click **Select one** and select the appropriate rights policy template.
   9. If desired, add an exception or audit configuration.
   10. Click **Save**.
   11. Repeat these steps to add additional transport protection rules.
5. Integrate the Exchange Data Loss Prevention feature with RMS
   1. Log on to Office 365 with an account with Office 365 Global Administrator permissions.
   2. From the Office 365 admin center, click the **Admin** drop down and select **Exchange**.
   3. Click **compliance management** and then click the **data loss prevention** tab.
   4. Click the plus icon and select **New DLP policy from template** to open the DLP policy from template wizard.
   5. Add a name and description.
   6. Select a template that matches the geographic region and vertical industry and click **Save**.
   7. Click the **mail flow** tab.
   8. Double click one of the rules that was created from the DLP policy above.
   9. Under the Do the following section, click the drop down, point to **Modify the message security** and **select Apply rights protection**.
   10. Select the appropriate rights policy template and click **OK**.
   11. Click **Save**.
   12. Repeat steps h through k to edit additional rules associated with the DLP policy.
   13. Repeat steps a through l to add additional DLP policies integrate with RMS.
6. Enabling Information Rights Management Functionality in SharePoint 2010/2013

*If your customer is not going to use IRM functionality in SharePoint 2010/2013, delete this section.*

The following steps are used to enable basic Information Rights Management (IRM) integration for Microsoft SharePoint Server 2010/2013. The corresponding SharePoint Server machines must be installed in a server with the Rights Management Services Client installed and configured like a normal client computer. Servers running SharePoint 2013 must be running the latest version of the RMS Client version 2.1. Servers running SharePoint 2010 must be running a version of the MSDRM client that includes support for RMS Cryptographic Mode 2. This version will depend on the operating system of the server running SharePoint 2010:

* Windows Server 2012 R2/Windows Server 2012: <http://www.microsoft.com/en-us/download/details.aspx?id=38396>
* Windows Server 2008 R2: <http://support.microsoft.com/kb/2627273>
* Windows Server 2008: <http://support.microsoft.com/kb/2627272>

1. Retrieve the Azure RMS URL for the tenant.
   1. Log on to a computer with the Azure AD Rights Management Administration Tool as a local administrator or equivalent.
   2. From the Start screen, enter **PowerShell** in the Search field.
   3. Right click the **PowerShell** icon and select **Run as administrator**.
   4. Type the following command and press **Enter**: **Import-module aadrm**
   5. Type the following command and press **Enter**: **Connect-aadrmService**
   6. Enter the user name and password of an Azure Active Directory Administrator account and press **Enter**.
   7. Type the following command and press **Enter**: Get-AadrmConfiguration
   8. The Microsoft RMS URL will be returned in a format that resembles the following example. Copy the URL for use when changing registry keys on the SharePoint servers: **https://5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com**
   9. Close Windows PowerShell and log off of the computer.
2. Modify the registry information to point to the RMS Connector
   1. Log on to the SharePoint server with an account with local administrative permissions or equivalent.
   2. From the Start menu, type **Regedit** in the Search Field and click **Registry Editor** to open the Registry Editor.
   3. Navigate to the following registry key: **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\MSIPC\ServiceLocation\LicensingRedirection**. If any keys within the path do not exist, create them.
   4. Create a new Reg\_SZ in the LicensingRedirection node and enter the URL copied in Step 1 as the Value.
   5. Double click the new Reg\_SZ and enter the URL of the RMS Connector in the Data field. Click **OK**.
   6. Close the Registry Editor and log off of the server.
   7. Repeat these steps for each SharePoint server that will use Azure RMS.
3. Enable SharePoint to use Azure RMS:
   1. Log on to a SharePoint server with an account that has **Full Control** over the document library.
   2. Click **Start**, type **SharePoint** in the Search field, and click **SharePoint 2013/2010 Central Administration**.
   3. Click **Security** and click **Configure information rights management**.
   4. Select **Use the default RMS server specified in Active Directory** and click **OK**
4. RMS protect a document library:
   1. Navigate to a SharePoint document library using credentials with **Full Control** over the document library.
   2. Click the **Page** tab and click **Library Settings**.
   3. Click **Information Rights Management**, located under the **Permissions and Management** column.
   4. Select the **Restrict permission to documents in this library on download** option.
   5. Enter a name and description for the permission policy.
   6. Optionally, you can select to allow users to print documents and access the content programmatically. You can also specify how often users must verify their credentials and specify when to stop applying permission to documents. Finally, you can select the option to block the upload of protected files. This option keeps the Azure RMS protection uniform for all documents in the library and enables SharePoint search and anti-virus capabilities.
   7. Click **OK.**
5. Enabling Information Rights Management Functionality in SharePoint Online

*If your customer is not going to use IRM functionality in SharePoint Online, delete this section.*

The following steps are used to enable basic Information Rights Management (IRM) integration for SharePoint Online.

1. Enable RMS integration with SharePoint Online
   1. Log on to Office 365 with an account with Global Administrator permissions.
   2. From the Office 365 Admin Center, click **Service settings** and then click the **Sites** tab.
   3. Click **View site collections and manage additional settings in the SharePoint Admin Center** to open the SharePoint Admin Center.
   4. Click **Settings**.
   5. In the Information Rights Management section, select the **Use the IRM service specified in your configuration option** and then click **OK**.
2. RMS protect a document library:
   1. Navigate to a SharePoint document library using credentials with **Full Control** over the document library.
   2. Click the **Page** tab and click **Library Settings**.
   3. Click **Information Rights Management**, located under the **Permissions and Management** column.
   4. Select the **Restrict permission to documents in this library on download** option.
   5. Enter a name and description for the permission policy.
   6. Optionally, you can select to allow users to print documents and access the content programmatically. You can also specify how often users must verify their credentials and specify when to stop applying permission to documents. Finally, you can select the option to block the upload of protected files. This option keeps the Azure RMS protection uniform for all documents in the library and enables SharePoint search and anti-virus capabilities.
   7. Click **OK**.
3. Enabling Information Rights Management Functionality in Windows Server 2012 R2/Windows Server 2012 FCI

*If your customer is not going to use IRM functionality in FCI, delete this section.*

The following steps are used to enable basic Information Rights Management (IRM) integration for FCI in Windows Server 2012 R2 and Windows Server 2012. The corresponding FCI machines must be installed in a server with the Rights Management Services Client installed and configured like a normal client computer.

1. Configure the FCI server to point to the RMS Connector.
   1. Log on to the FCI server with local administrative permissions or equivalent.
   2. From the Start Menu type **Regedit** in the Search Field and click **Registry Editor** to open the Registry Editor.
   3. Navigate to the following registry key: **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\MSDRM**.
   4. Right click the **MSDRM** node, point to **New**, and select **Key**.
   5. Enter **ServiceLocation**.
   6. Right click **ServiceLocation**, point to **New** and select **Key**.
   7. Enter **EnterprisePublishing**.
   8. Double click the **Default** Reg\_SZ to open the Edit String dialog box.
   9. Enter the following value in the field and click OK: **http://***ConnectorFQDN***/\_wmcs/licensing**
   10. Close the Registry Editor.
   11. Log off.
2. Create classification properties to be assigned to documents:
   1. Log on to the FCI server as an administrator.
   2. In Server Manager, click **Tools** and select **File Server Resource Manager** to open the File Server Resources Manager.
   3. Expand **Classification Management** and click **Classification Properties**.
   4. Click New Classification Property. Configure the classification property as desired.
   5. Repeat this step for all classification properties that must be created.
3. Create classification rules that assign classification properties to documents stored in a particular location or containing particular content:
   1. Log on to the FCI server as an administrator.
   2. In Server Manager, click **Tools** and select **File Server Resource Manager** to open the File Server Resources Manager.
   3. Expand **Classification Management** and click Classification Rules.
   4. Click New Classification Rule. Configure the classification as desired.
   5. Repeat this step for all classification rules that must be created.
4. Create file management tasks to protect documents that contain particular properties with Azure RMS:
   1. Log on to the FCI server as an administrator.
   2. In Server Manager, click **Tools** and select **File Server Resource Manager** to open the File Server Resources Manager.
   3. Click File Management Tasks and in the Actions pane, click **Create File Management Task** to open the Create File Management Task dialog box.
   4. Enter a name in the Task name field and enter a corresponding description.
   5. Click the **Scope** tab. Select the desired scope for this task.
   6. Click the **Action** tab. Under the Type drop down, select **RMS Encryption**. Select a rights policy template or create a protection policy.
   7. Select the **Condition** tab and click **Add** to open the Property Condition dialog box.
   8. Add the appropriate conditions.
   9. Click the **Schedule** tab and select the desired schedule. Click **OK**.
   10. Repeat these steps for all file management tasks that must be created.