Solution Test Plan



Information Protection Using Azure Rights Management Services

Prepared for

[Customer Name]

June 20, 2014

Version

Prepared by

**Author**

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 Objectives 7](#_Toc391033079)

[1.1 Testing Tools 7](#_Toc391033080)

[2 Deployment Test 8](#_Toc391033081)

[2.1 Test Methodology 8](#_Toc391033082)

[2.2 Verifying Azure Rights Management Services Functionality – Details 9](#_Toc391033083)

[2.2.1 Verifying Intranet Client Functionality – Details 9](#_Toc391033084)

[2.2.2 Verifying Internet Azure Rights Management Services Client Functionality – Details 14](#_Toc391033085)

[3 Functional Tests 17](#_Toc391033086)

[3.1 Solution Use Cases 17](#_Toc391033087)

[3.2 Before the tests 28](#_Toc391033088)

[3.3 Test Methodology 29](#_Toc391033089)

[4 Appendix A: Azure Rights Management Services Network Communication Dataflow 29](#_Toc391033090)

[4.1 RMS Architecture – Data Flow Required for Base Architecture 29](#_Toc391033091)

[4.1.1 RMS Architecture – Data Flow Required for Trusted User Domains – Business to Business (B2B) 32](#_Toc391033092)

[4.1.2 RMS Architecture – Data Flow Required for Trusted User Domains – Intra-organization 32](#_Toc391033093)

[4.1.3 RMS Architecture – Data Flow Required for Trusted Publishing Domains – Internal 33](#_Toc391033094)

[4.1.4 RMS Architecture – Data Flow Required for Federation Trust – Business to Business 34](#_Toc391033095)

**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. Objectives

This document contains the test plan for the solution for . This test plan is developed based on a solution design created by the project team based on the requirements and business goals, and the deployment strategy devised for rolling out this solution.

The proposed test plan comprises deployment tests and functional tests:

* **Deployment Tests** validate the overall deployment strategy by testing the actual deployment checklists and scripts. It also confirms that the team is familiar with all steps of the deployment process as the team walks through it in a test environment.
* **Functional Tests** will cover all functionality defined by the solution design. The purpose of these tests is to verify that the proposed Azure Rights Management Services usage for each business scenario will work as expected.

Keep the following paragraph if the customer requested performance tests.

The testing tools and the testing methodology are presented in the following sections, as are thorough descriptions of the test scenarios and explanations of how they can be conducted in the lab environment. A separate check sheet is used to record the test results and other comments.

* 1. Testing Tools

The following software tools will be used during testing:

* **Ping/Telnet/DNSLookup**

These tools enable an administrator to validate the configuration of the supporting components in the Azure Rights Management Services architecture using the appropriate virtual name, fully qualified domain name (FQDN) and the respective TCP/IP ports.

* **Microsoft**  **Internet Explorer**

By default, Azure Rights Management Services Servers have the HTTP VERB GET allowed in the Microsoft Internet Information Services (IIS) service configuration. This allows specific Azure Rights Management Services Web Services that test the connectivity and authentication parameters to be placed directly into the Internet Explorer (IE) toolbar.

* **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. Deployment Test

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

The deployment test validates the deployment plan by walking through the deployment process in a test environment. Besides ensuring the deployment plan will work as expected, this test also provides the opportunity togain experience and become familiar with each step of the deployment process.

* 1. Test Methodology

The test covers the most important phases of the Deployment Plan, from the initial lab configuration up to the point that all systems are in the Azure Rights Management Services (Azure RMS) solution, and covering all deployment steps performed in between. The following phases will be evaluated in the deployment tests:

1. Prepare the Environment - Architecture Prerequisites
2. Prepare the Environment - Groups and Policies and Active Directory Components
3. Synchronize Directories
4. Enable Azure RMS and License Users
5. Configure Azure Rights Management Services Architecture and Templates
6. Implement additional Azure Rights Management Services Components (RMS Connector)
7. Implement Azure Rights Management Services Client Components
8. Implement Azure RMS integration with other servers

The test proceeds by executing each phase of the deployment plan independently, and then running the appropriate validation steps.

The steps to perform for the deployment test are those indicated in the Solution Deployment Plan document. The same document includes the Validation tests at the end of each step where applicable.

After the deployment tests, some core infrastructure tests will be performed to validate correct behavior of the infrastructure.

* 1. Verifying Azure Rights Management Services Functionality – Details

To perform the functional tests, the following steps should be taken for each use case scenario.

Before configuring RMS, validate that all prerequisites have been configured.

* + 1. Verifying Intranet Client Functionality – Details

This section evaluates the appropriate client functionality when interacting/using the Azure Rights Management Services service.

* + - 1. Client Functional Test – Protecting a Microsoft Office Word 2013 Document

*If your customer is not using Office 2013 replace this section with similar instructions for Office 2010 as needed.*

Validate document protection functionality by protecting a document and assigning rights to an Azure Rights Management Services Group using Microsoft Office Word 2013.

1. Log on to test computer with a valid Active Directory user ID.
2. Click **Start**, point to **All Programs**, point to **Microsoft Office**, and then click **Microsoft Office Word 2013**.
3. On the blank page, type **This is a rights-protected document**.
4. Click **File**, click **Protect Document**, click **Restrict Access**, and click **Restricted Access** to open the Permission dialog box.
5. In the **Permission** dialog box, select the **Restrict permission to this document** check box.
6. In the **Read** field, type the email address of a test group defined in the lab.
7. Click **More Options**.
8. Under **Additional Permissions for Users**, select the **This document expires on** check box.
9. Click the drop-down menu and click next Sunday’s date.
10. Select the **Require a connection to verify user’s permission** check box.
11. Click **OK** to close the **Permission** dialog box.
12. Click **Save As**.
13. Save the file as the following: **C:\Files\1stRMSTest.docx**
14. Close Microsoft Office Word 2013.
    * + 1. Client Functional Test – Consuming a Microsoft Office Word 2013 Document

*If your customer is not using Office 2013 replace this section with similar instructions for Office 2010 as needed.*

Validate users can consume RMS-protected content by consuming a document and validating your rights using Microsoft Office Word 2013.

1. Log on to test computer with a valid Active Directory user ID that belongs to the group assigned access in previous test.
2. Open File Explorer.
3. Browse to **C:\Files\** and double click **1stRMSTest.docx** to open Microsoft Word.
4. At the Microsoft Office prompt, read the message stating that the document is restricted. Click **OK**. A message will appear, stating that the system is verifying your credentials for opening restricted content.
5. When the document opens, click **File** and verify that the Print and Save options are not available.
6. In the **Restricted Access banner**, click **View Permission**, and then validate the rights assigned to that user.
7. Notice the listing of granular permissions. The user has been restricted to being able only to view the document. The document will also expire “next Sunday”.
8. Click **OK** to close the **Permission** dialog box.
9. Close Microsoft Office Word 2013.
10. Close all windows.
    * + 1. Client Functional Test – Exchanging Protected E-mail using Microsoft Office Outlook 2013

Validate that users can protect and consume RMS-protected e-mail messages. Perform the following steps with UserA.

1. Log on to test computer with a valid Active Directory user ID.
2. Open Microsoft Outlook 2013.
3. Click **New Email** to compose a new e-mail message.
4. In the **To** box, type **UserB**.
5. On the **Subject line**, type **Azure Rights Management Services** **E-mail Test**.
6. In the body of the message, type **First Azure Rights Management Services E-mail Test!**
7. Click the **Options** tab, click the **Permission** drop down menu, and select **Do Not Forward**.
8. After a few moments, a banner appears at the top of the e-mail message stating that the message has been applied with the Do Not Forward template.
9. Click **Send**. Make sure that the message exits the Outbox before continuing.
10. CloseMicrosoft Outlook and then log off from CLI01.

Perform the following steps with UserB.

1. Log on as UserB.
2. Open Microsoft Outlook 2013.
3. Notice the message from UserA. Also notice that the message cannot be viewed in the reading pane until your credentials have been verified.
4. Double-click the message from UserA.
5. In the Microsoft Office dialog box, read the information provided, select **Don’t show this message again** and then click **OK**.
6. At the Microsoft Office prompt, read the message stating that the document is restricted. Click **OK**.
7. After a few moments, the message opens. Notice the **Do Not Forward** banner.
8. When the message opens, click the **File** menu. Verify that the Print and Save options are not available and that you cannot forward or copy the e-mail content.
9. Close the e-mail message and close Microsoft Outlook.
10. Close all windows.
    * + 1. Client Functional Test – Using Azure Rights Management Services Templates

Validate that users can protect and consume RMS-protected documents using Rights Policy Templates.Perform the following steps with UserA.

1. Log on to test computer with a valid Active Directory user ID.
2. Open Microsoft Office Word 2013.
3. Type the following text in the new document:

**This is a document that should not be altered by anyone besides the author.**

1. Click File, click **Protect Document**, click **Restrict Access**, and select a template that already has been deployed.
2. Save the document as **C:\Files\4AnyoneRead.doc**, and then close Office Word.
3. Log off.

Perform the following steps with UserB.

1. Log on as UserB.
2. Click **Start** and then click **Microsoft Office Word**.
3. Start **Windows Explorer**, browse to **C:\Files**, and then open the **4AnyoneRead.doc** file.
4. At the **Microsoft Office** prompt, click **OK**. Attempt to print or save the document*.*
5. Close Office Word, and then close all open windows.
   * + 1. Client Functional Test – Trying to Access a Document Without Explicit Rights

Validate that unauthorized users cannot consume RMS-protected documents. Perform the following steps with UserC.

1. Log on to test computer with a valid Active Directory user ID.
2. Start Microsoft Office Word 2013.
3. Start **Windows Explorer**, browse to **C:\Files**, and then open the **1stRMSTest.docx** file. The following message appears:

*This file has permission only for users other than the user logged in on the PC.*

Note that the user cannot open the file because the user is not listed as a user with the appropriate assigned permissions or as belonging to a group with assigned permissions. This prevents the message from being read by unauthorized users to whom the author may have inadvertently sent the message.

1. Close Office Word.
   * + 1. Client Functional Test – Using the RMS App to Protect Text and Image Files

Validate that users can create and consume protected text and image files using the RMS App. Perform the following steps with UserA

1. Log on to test computer with a valid Active Directory user ID.
2. Open Windows Explorer and browse to **C:\Files**.
3. Create a new text document.
4. Open the text document in Notepad and add some text.
5. Click **File**, click **Save**, and save the document as **C:\Files\Protected Text File**.
6. Close Notepad.
7. Select and right click the new text file, point to **Protect in Place**, and select **Custom** **Permissions** to open the Add Protection dialog box.
8. If you are asked for credentials, enter the user name and password of the test user account.
9. Enter the email address of UserB in the Users field.
10. In the permissions slider bar, select **Viewer** and click **Apply**.
11. Verify that the icon for the text document has changed and that the file type is now a protected text document.
12. Close all open windows and log off of the computer.

Perform the following steps as UserB.

1. Log on to test computer with a valid Active Directory user ID.
2. Open Windows Explorer and browse to **C:\Files**.
3. Double click **Protected Text File** to open the protected text file.
4. Verify that you are not able to print, edit, or save the content.
5. Close the RMS App Viewer.
6. Close all open windows and log off of the computer.
   * + 1. Client Functional Test – Using the RMS App to Protect Generic Files

Validate that users can create and consume protected files of any file type using the RMS App. Perform the following steps with UserA

1. Log on to test computer with a valid Active Directory user ID.
2. Open Windows Explorer and browse to C:\Files.
3. Select and right click a file of generic file type, point to Protect in Place, and select Custom Permissions to open the Add Protection dialog box.
4. If you are asked for credentials, enter the user name and password of the test user account.
5. Enter the email address of UserB in the Users field.
6. In the permissions slider bar, select **Viewer** and click **Apply**.
7. Verify that the file type is now a pfile.
8. Close all open windows and log off of the computer.

Perform the following steps as UserB.

1. Log on to test computer with a valid Active Directory user ID.
2. Open Windows Explorer and browse to **C:\Files**.
3. Double click the generic file you saved in the previous step to open the Protected File dialog box.
4. Review the permissions you have been assigned and click Open.
5. Verify that the file opens in its native application and that granular level permissions are not enforced.
6. Close all open windows and log off of the computer.
   * + 1. Client Functional Test – Converting Documents in Non-RMS-Enabled Applications to XPS

Validate document conversion to XPS and assign Active Directory Rights Management Services permissions using Azure Rights Management Services Templates. Perform the following steps with UserC.

1. Log on to test computer with a valid Active Directory user ID.
2. Open an Adobe Acrobat Reader file (PDF).
3. Press **CTRL+P**.
4. For the printer name, point to **Microsoft XPS Document Writer** and click **Properties**.
5. In **Microsoft XPS Document Writer Properties,** select the checkbox called **Automatically open XPS documents using the XPS viewer**, and then click **OK**.
6. In the **Save the File As** window**,** assign to the file the following name and location: **C:\Information Protection using Active Directory Rights Management Services – XPS Testv1.0.xps**.
7. The XPS file appears inside Internet Explorer.
8. Click the **Permissions** button.
9. Inside the **Permissions** window**,** select **Apply Permissions** and then click the icon presented beside the **Add User** button. This will assign the **Everyone** group the rights to read the XPS document.
10. Click the **Save** Button.
11. Validate that the XPS file is rights-protected.
12. Close Internet Explorer.
13. Close Adobe Reader.
14. Log off.
    * + 1. Client Functional Test – Validate Azure Rights Management Services Configuration Settings

Validate Client configuration settings using the IRMDiagnosticsTool.

1. Log on to test computer with a valid Active Directory user ID.
2. Access the path where **IRMDiagnosticsTool** has been installed.
3. Double click **IRMDiagnosticsTool**.to launch the tool.
4. Click **Advanced Mode**. Click **File** and select **Scan Machine**.
5. Validate in the Default Server Settings section that the presented values point to the Azure Rights Management Services service, and validate you have the service working as expected (protect and consume documents).
6. Validate that you have the appropriate certificates (**GIC/CLC**) to use RMS.
7. Validate that the RMS registry information is accurate with configuration settings propagated by GPO or manually configured in the workstation. Ignore errors regarding the Office version.
8. Close all windows.
9. Log off.
   * 1. Verifying Internet Azure Rights Management Services Client Functionality – Details

The following test should be performed by using a computer outside the corporate network that is trying to access the Azure Rights Management Services service.

* + - 1. Client Functional Test – Protect a Document from the Internet Using a Computer Already Activated

Validate that users on a computer with Azure Rights Management Services already activated can protect documents without needing to contact the Azure Rights Management Services service.

1. Log on to internal computer connected to the Internet (typically a laptop computer).
2. Open **Microsoft Office Word 2013**.
3. On the blank page, type **This is a rights-protected document from the Internet.**
4. Click **File**, click **Protect Document**, click **Restrict Access**, and click **Restricted Access** to open the Permission dialog box.
5. In the **Permission** dialog box, select the **Restrict permission to this document** check box.
6. In the **Read** field, type the email address of a test group defined in the lab.
7. Click **More Options**
8. Select the **Require a connection to verify user’s permission** check box.
9. Click **OK** to close the **Permission** dialog box.
10. Click **Save As**.
11. Save the file as the following: **C:\Files\Internet\_RMSTest.docx**
12. Close Microsoft Office Word 2013.
13. Log off.

To access a protected document from the Internet, perform the following steps:

1. Log on to an internal computer connected to the Internet with another user that already reads and protects content in that computer (RMS already activated).
2. Open Windows Explorer.
3. Browse to **C:\Files\** and then select ***InternetRMSTest.docx***. Click **Open**. At the Microsoft Office prompt, read the message stating that the document is restricted. Click **OK.**A message appears, saying that the system is verifying your credentials for opening restricted content.
4. When prompted, provide your credentials.
5. When the document opens, click **File** and verify that the Print and Save options are NOT available.
6. In the **Restricted Access** banner, click **View permission**, and then validate the rights assigned to that user.
7. Click **OK** to close the **Permission** dialog box.
8. Close Microsoft Office Word 2013.
9. Close all windows.
10. Log off.
    * + 1. Client Functional Test – Protect and Consume a Document from the Internet Using a Non-Domain-Joined Computer

Validate that users in a non-domain-joined computer can protect and consume documents by contacting the Azure Rights Management Services service and providing their Azure Active Directory credentials. Validate that you have already configured the registry settings to contact your certification and licensing clusters.

1. Log on to a non-domain-joined computer connected to the Internet (typically a laptop computer).
2. Open **Microsoft Office Word 2013**.
3. On the blank page, type **This is a rights-protected document from the Internet.**
4. Click **File**, click **Protect Document**, click **Restrict Access**, and click **Restricted Access** to open the Permission dialog box.
5. In the **Permission** dialog box, select the **Restrict permission to this document** check box.
6. In the **Read** field, type the email address of a test group defined in the lab.
7. Click **More Options**
8. Select the **Require a connection to verify user’s permission** check box.
9. Click **OK** to close the **Permission** dialog box.
10. Click **Save As**.
11. Save the file as the following: **C:\Files\Internet\_RMSTest2.docx**
12. Close Microsoft Office Word 2013.
13. Log off.

To consume an Azure Rights Management Services document using a non-domain-joined computer, perform the following steps.

1. Log on to a non-domain-joined computer connected to the Internet with another user that already reads and protects content in that computer (RMS already activated).
2. Open Windows Explorer.
3. Browse to **C:\Files\** and then select ***InternetRMSTest2.docx***. Click **Open**. At the Microsoft Office prompt, read the message stating that the document is restricted. Click **OK.**A message appears, saying that the system is verifying your credentials for opening restricted content.
4. When prompted, provide your credentials.
5. When the document opens, click **File** and verify that the Print and Save options are NOT available.
6. In the **Restricted Access** banner, click **View permission**, and then validate the rights assigned to that user.
7. Click **OK** to close the **Permission** dialog box.
8. Close Microsoft Office Word 2013.
9. Close all windows.
10. Log off.
    * + 1. Client Functional Test – Consume a Document from the Internet Using a Non-Domain-Joined Computer

To validate that users on a non-domain-joined computer can protect and consume e-mail messages by using Outlook Web Access, contacting the Azure Rights Management Services service, and providing their Azure Active Directory credentials, perform the following steps.

1. Log on to internal computer connected to the Internet (typically a laptop computer).
2. Click **Start** and then click **Internet**. Internet Explorer opens.
3. Connect to your Outlook Web Access Server; provide the credentials using a valid user.
4. Access a protected message. A message appears inside the e-mail body that says the message has been received with restricted permissions.
5. Validate the content of this Azure Rights Management Services protected e-mail message.
6. Right-click the protected document and then select **Permissions**.
7. Validate the use permissions.
8. Close all windows.
9. Log off.
10. Functional Tests

After initially deploying the solution successfully in a pre-production or limited production environment, the deployment team will perform basic functionality tests to validate the configuration before rolling into production. These tests will be performed by IT personnel on the pre-production or limited production environment after initial rollout.

These tests will be scripted based on the use case lists below.

There are XXX use cases (Use case 1, Use case 2, [...]) defined in the solution and listed in the table below. For each use case, a normal user (without administrative privileges on the computer or the Azure RMS subscription) should go through the steps indicated and validate the results. Any deviation from the expected results should be documented and analyzed with the project team. If required, changes to the configuration will be made until the results are satisfactory and according to the expectations and according to the capabilities of the technology.

Once these tests have been completed successfully, the solution will be rolled out in production to a limited group of production users. These users will be enrolled to perform tests on the solution. The tests performed by these users will not be scripted as they will be natural operations performed according to their daily needs, in order to validate both the technology and its usability and applicability to the real-world scenarios.

* 1. Solution Use Cases

The functional tests will be conducted based on the communication paths described in the following scenarios. The functional tests will verify whether all valid common documentation protection and consumption capabilities deploy as expected under the solution, and will verify that application-level functionality and user experiences are not adversely affected.

*Note: Customize the test case table below according to your customer’s use cases. Cases provided only as an example. Duplicate all template-related tests for each template to be used and specify the expected results for the different user groups with each. If multiple versions of Office are going to be used, also indicate that the tests must be performed on each platform. In a multi-forest environment add use cases for protection and consumption of content between forests. If extranet access by external users is included, add use cases for such scenarios as needed.*

| **Test Case No.** | **Test Case Description** | Test Case Procedures | Expected Results |
| --- | --- | --- | --- |
|
|  |
| DOC-T1 | Protect document with ad-hoc rights from uninitialized client | On a machine that has not used Azure RMS before, create document in MS Word (2010 Professional Plus, or 2013 Professional Plus). Use the menus or ribbon to select "Restricted Access" option. Select the check box for "Restrict Permission to this Document". Enter an email address in the Read Only box for a valid user. Click OK, save the file. | Client should ask for RMS initialization or directly proceed to initialize client. Initialization should take less than ten seconds. User should be prompted to supply Azure Active Directory credentials. User should be able to pick users from the GAL as recipients of rights. Document should be protected but author should have full rights. |
| DOC-T2 | Protect document with template from uninitialized client | On a machine that has not used Azure RMS before, create document in MS Word (2010 Professional Plus, or 2013 Professional Plus). Use the menus or ribbon to select a previously created RMS template that assigns read rights to a group (not individual user). Save the file. | Client should see the templates in the Office menus after RMS initialization. Client should ask for RMS initialization or directly proceed to initialize client. Initialization should take less than ten seconds. User should be prompted to supply Azure Active Directory credentials. Document should be protected but author should have full rights. |
| DOC-T3 | Protect document with ad-hoc rights from initialized client | On a machine that has used Azure RMS before, create document in MS Word (2010 Professional Plus, or 2013 Professional Plus). Use the menus or ribbon to select "Restricted Access" option. Select the check box for "Restrict Permission to this Document". Enter an email address in the Read Only box for a valid user. Click OK, save the file. | For a domain-member machine no credential prompts should occur. User should be able to pick users from the GAL as recipients of rights. Document should be protected immediately but author should have full rights. |
| DOC-T4 | Protect document with template from initialized client | On a machine that has used Azure RMS before, create document in MS Word (2010 Professional Plus, or 2013 Professional Plus). Use the menus or ribbon to select a previously created RMS template that assigns read rights to a group (not individual user). Save the file. | Client should see the templates in the Office menus. For a domain-member machine no credential prompts should occur. Document should be protected but author should have full rights. |
| DOC-T5 | Open protected document (ad hoc protection) from file system in an uninitialized client. | From an uninitialized client logged in as the user that was granted rights in RMS-T1, double click on the file protected in RMS-T1. Repeat same step from an uninitialized client but logged on as a different, unauthorized user. | Logged in as authorized client, user should automatically acquire rights for the document. User may be prompted to supply Azure Active Directory credentials and may see a prompt asking if the user wants to connect to Azure RMS to acquire rights. Once license has been acquired, user should see the contents of the document but not be able to copy, edit or print the file.  An unauthorized user should not be able to open the file. |
| DOC-T6 | Open protected document (ad hoc protection) from email in an uninitialized client. | Send the file protected in RMS-T1 via email to the user that was granted rights in RMS-T1. From an uninitialized client logged in as that user double click on the attachment. Repeat same step from an uninitialized client but logged on as a different, unauthorized user. | Logged in as authorized client, user should automatically acquire rights for the document. User may be prompted to supply Azure Active Directory credentials and may see a prompt asking if the user wants to connect to Azure RMS to acquire rights. Once license has been acquired, user should see the contents of the document but not be able to copy, edit or print the file.  An unauthorized user should not be able to open the file. |
| DOC-T7 | Open protected document (template) in an uninitialized client. | From an uninitialized client logged in as a user with read rights in the template used in RMS-T2, double click on the file protected in RMS-T2. Repeat same step from an uninitialized client but logged on as a different, unauthorized user. | Logged in as authorized client, user should automatically acquire rights for the document. User may be prompted to supply Azure Active Directory credentials and may see a prompt asking if the user wants to connect to Azure RMS to acquire rights. Once license has been acquired, user should see the contents of the document but not be able to copy, edit or print the file, according to the rights specified in the template. User should see a banner at the top of the document explaining the limitations imposed by the template, as included in the template definition. The banner should be in the same language used for the client, if that language is defined for the template. An unauthorized user should not be able to open the file. |
| DOC-T8 | Open protected document from uninitialized unmanaged client | From an uninitialized unmanaged client logged in as the user that was granted rights in RMS-T1, double click on the file protected in RMS-T1. Repeat same step from an uninitialized client but logged on as a different, unauthorized user. | If the machine or user has the registry keys set to configure RMS to use the right certification URLs, logged in as authorized client, user should automatically acquire rights for the document. User may be prompted to supply Azure Active Directory credentials and may see a prompt asking if the user wants to connect to Azure RMS to acquire rights. Once license has been acquired, user should see the contents of the document but not be able to copy, edit or print the file.  An unauthorized user should not be able to open the file.  If the machine is using Office 2010 and the necessary script has not been deployed, the operation should fail or the user should see prompts to use Windows Live ID for RMS activation, which should fail. |
| APP-T1 | Protect text or image file with ad-hoc rights from uninitialized client | On a machine that has not used Azure RMS before, create a text or image file. Use right click option in Windows Explorer to select the "Protect in-place" option and select “Custom Permissions”. Enter an email address in the Users field for a valid user. Select Viewer permissions and click Apply. | Client should ask for RMS initialization or directly proceed to initialize client. Initialization should take less than ten seconds. User should be prompted to supply Azure Active Directory credentials. User should be able to enter a user by email address. File should be protected but author should have full rights. |
| APP-T2 | Protect text or image file with a rights policy template from uninitialized client | On a machine that has not used Azure RMS before, create a text or image file. Use right click option in Windows Explorer to select the "Protect in-place" option and select a rights policy template. | Client should ask for RMS initialization or directly proceed to initialize client. Initialization should take less than ten seconds. User should be prompted to supply Azure Active Directory credentials. File should be protected but author should have full rights. |
| APP-T3 | Protect text or image file with ad-hoc rights from initialized client | On a machine that has used Azure RMS before, create a text or image file. Use right click option in Windows Explorer to select the "Protect in-place" option and select “Custom Permissions”. Enter an email address in the Users field for a valid user. Select Viewer permissions and click Apply. | No credential prompts should occur. User should be able to enter a user by email address. File should be protected but author should have full rights. |
| APP-T4 | Protect text or image file with a rights policy template from uninitialized client | On a machine that has used Azure RMS before, create a text or image file. Use right click option in Windows Explorer to select the "Protect in-place" option and select a rights policy template. | Client should see the templates in the Windows Explorer menus. No credential prompts should occur. Document should be protected but author should have full rights |
| APP-T5 | Open protected text or image file (ad hoc protection) from file system in an uninitialized client. | From an uninitialized client logged in as the user that was granted rights in APP-T1, double click on the file protected in APP-T1. Repeat same step from an uninitialized client but logged on as a different, unauthorized user. | Logged in as authorized client, user should automatically acquire rights for the document. User may be prompted to supply Azure Active Directory credentials and may see a prompt asking if the user wants to connect to Azure RMS to acquire rights. Once license has been acquired, user should see the contents of the file in the RMS Viewer but not be able to copy, edit or print the file.  An unauthorized user should not be able to open the file. |
| APP-T6 | Open protected file (template) in an uninitialized client. | From an uninitialized client logged in as a user with read rights in the template used in APP-T2, double click on the file protected in APP-T2. Repeat same step from an uninitialized client but logged on as a different, unauthorized user. | Logged in as authorized client, user should automatically acquire rights for the document. User may be prompted to supply Azure Active Directory credentials and may see a prompt asking if the user wants to connect to Azure RMS to acquire rights. Once license has been acquired, user should see the contents of the file in the RMS App Viewer but not be able to copy, edit or print the file, according to the rights specified in the template. User should see a banner at the top of the file explaining the limitations imposed by the template, as included in the template definition. The banner should be in the same language used for the client, if that language is defined for the template. An unauthorized user should not be able to open the file. |
| APP-T7 | Open protected text or image file (ad hoc protection) from file system in an initialized client. | From an initialized client logged in as the user that was granted rights in APP-T3, double click on the file protected in APP-T3. Repeat same step from an uninitialized client but logged on as a different, unauthorized user. | Logged in as authorized client, user should automatically acquire rights for the document. User should not be prompted to supply Azure Active Directory credentials but may see a prompt asking if the user wants to connect to Azure RMS to acquire rights. Once license has been acquired, user should see the contents of the file in the RMS App Viewer but not be able to copy, edit or print the file.  An unauthorized user should not be able to open the file. |
| APP-T8 | Open protected file (template) in an initialized client. | From an initialized client logged in as a user with read rights in the template used in APP-T4, double click on the file protected in APP-T4. Repeat same step from an uninitialized client but logged on as a different, unauthorized user. | Logged in as authorized client, user should automatically acquire rights for the document. User should not be prompted to supply Azure Active Directory credentials but may see a prompt asking if the user wants to connect to Azure RMS to acquire rights. Once license has been acquired, user should see the contents of the file in the RMS App Viewer but not be able to copy, edit or print the file, according to the rights specified in the template. User should see a banner at the top of the file explaining the limitations imposed by the template, as included in the template definition. The banner should be in the same language used for the client, if that language is defined for the template. An unauthorized user should not be able to open the file. |
| APP-T9 | Protect a generic file with wrapper-based protection from initialized client | On a machine that has used Azure RMS before, create a file in a format other than Office, PDF, XPS, TXT, or image. Use right click option in Windows Explorer to select the "Protect in-place" option and select a rights policy template. | Client should ask for RMS initialization or directly proceed to initialize client. Initialization should take less than ten seconds. User should be prompted to supply Azure Active Directory credentials. User should be able to enter a user by email address. File should be protected but author should have full rights. |
| APP-T10 | Open protected generic file (template) in an initialized client. | From an initialized client logged in as a user with read rights in the template used in APP-T9, double click on the file protected in APP-T9. In the RMS App dialog box, click Open.  Repeat same step from an uninitialized client but logged on as a different, unauthorized user. | Logged in as authorized client, user should automatically acquire rights for the document. User should not be prompted to supply Azure Active Directory credentials but may see a prompt asking if the user wants to connect to Azure RMS to acquire rights. Once license has been acquired, user should see the contents of the file in the native application and no granular-level permissions should be enforced.  An unauthorized user should not be able to open the file. |
| APP-11 | Protect and share an image from a mobile device | From a mobile device (Windows, iOS, or Android) that has the RMS App installed on it, open the RMS App. Choose a picture from the library or take a new picture. Select a rights policy template and click Apply. | Client should ask for RMS initialization or directly proceed to initialize client. Initialization should take less than ten seconds. User should be prompted to supply Azure Active Directory credentials. User should be able to select a rights policy template. User should be able to share the image using email or other application. |
| APP-12 | Open a protected file from a mobile device | From an initialized client, create a protected text or image file and email it to an authorized user.  From a mobile device (Windows, iOS, or Android) that has the RMS App installed on it, open the email containing the protected attachment. Click the attachment and select to open the file in the RMS App.  Repeat same step from an uninitialized client but logged on as a different, unauthorized user. | Logged in as authorized client, user should automatically acquire rights for the document. User may be prompted to supply Azure Active Directory credentials. Once license has been acquired, user should see the contents of the file in the RMS App Viewer but not be able to copy, edit or print the file, according to the rights specified in the template. An unauthorized user should not be able to open the file. |
| EML-T1 | Protect email with Do Not Forward option from initialized client | On a machine that has used Azure RMS before, create an email in Outlook (2010 Professional Plus, or 2013 Professional Plus) and address it to a specific group and an individual user. Add unprotected office attachments to the email (generic documents with some test content). Use the menus or ribbon to select "Do Not Forward" option. Click Send. | There should be no delay or credential prompts. For a domain-member machine no credential prompts should occur. |
| EML-T2 | Protect email with template from initialized client | On a machine that has used Azure RMS before, create an email in Outlook (2010 Professional Plus or 2013 Professional Plus) and address it to the different groups specified in the template, as well as to a user without rights granted in the template. Add unprotected office attachments to the email (generic documents with some test content). Use the menus or ribbon to select the desired Rights Policy Template. Click Send. | User should be able to see the different templates listed. There should be no delay or credential prompts. For a domain-member machine no credential prompts should occur. |
| EML-T3 | Open protected email (DNF) in an initialized client. | From an initialized client logged in as the individual recipient of the email in EML-T1, double click on the email protected in EML-T1. Try to perform actions on the email aimed at extracting data such as copying or printing. Open each of the attachments in turn and perform the same tests. Repeat same step logged on as a user that's a member of the recipient group. | Logged in as either user, user should automatically acquire rights for the email. User shouldn't see credential prompts or other messages other than a prompt asking if the user wants to connect to Azure RMS to acquire rights. Once license has been acquired, user should see the contents of the mail but not be able to copy, edit or print the file. Forward options should be disabled. User should be able to open the attachments but not to copy, print or otherwise extract data. |
| EML-T4 | Open protected email (Template) in an initialized client. | From an initialized client logged in as different users with and without rights on the rights policy template used in EML-T2, double click on the email protected in EML-T2. Try to perform actions on the email aimed at extracting data such as copying or printing. Open each of the attachments in turn and perform the same tests. | Logged in as a user with rights assigned on the template, the user should automatically acquire rights for the document. User shouldn't see credential prompts or other messages other than a prompt asking if the user wants to connect to Azure RMS to acquire rights. Once license has been acquired, user should see the contents of the document but see the limitations defined in the template for the groups the user is a member of. The user should see the same limitations on the attachments. As an unauthorized user should not be able to open the mail or the attachments. |
| EML-T5 | Open prelicensed email from an initialized client while offline. | From an initialized client logged in as the individual recipient of the email in EML-T1, download the email and then disconnect from the network. Double click on the email protected in EML-T1. Open each of the attachments in turn. | The user should be able to open the email and the attachments with restricted permissions, even if the user is not connected to the network. |
| SPS-T1 | Download a document from a protected SharePoint library | From an initialized client logged in as a user with contribute rights over a protected SharePoint library, upload an unprotected document to the library. Then download the same document from the library as that user and as another user with read-only rights on the library. Both users forward the document via any storage media to the other user and try to open it. | Either user should be able to download the document. Both users should receive a document that's RMS-protected with an ad-hoc policy. The user with contribute rights should be granted edit and copy rights over the document, the other user should have read-only rights over the downloaded document. Neither user should be able to open the document downloaded by the other user. |
| FCI-T1 | Protect document stored on a file server automatically | On a machine that has used Azure RMS before and has Work Folders enabled, create a document in MS Word (2010 Professional Plus or 2013 Professional Plus) containing a key word or phrase specified as sensitive in FCI. Save the file on the file server. | Within a couple of minutes, refresh File Explorer and open the document. It will be RMS-protected with the appropriate rights policy template applied. |
| FCI-T2 | Automatically protect document synchronized with Work Folders and stored on a file server | On a machine that has used Azure RMS before and has Work Folders enabled, create a document in MS Word (2010 Professional Plus or 2013 Professional Plus) containing a key word or phrase specified as sensitive in FCI. Save the file in the Work Folders container. | Within a couple of minutes, refresh the Work Folders container and open the document. It will be RMS-protected with the appropriate rights policy template applied. |
| OWA-T1 | Protect email with Do Not Forward option from OWA | On a machine that doesn't have the RMS client installed, use a supported browser to connect to OWA in an Exchange 2013/2010 server, create an email and address it to a specific group and an individual user. Add unprotected office attachments to the email (generic documents with some test content). Use the menus or ribbon to select "Do Not Forward" option. Click Send. | User should be able to apply protection and send the email. |
| OWA-T2 | Protect email with template from OWA | On a machine that doesn't have the RMS client installed, use a supported browser to connect to OWA in an Exchange 2013/2010 server, create an email and address it to a specific group and an individual user. Add unprotected office attachments to the email (generic documents with some test content). Use the menus or ribbon to select the desired RMS template. Click Send. | User should see the templates in OWA and apply them. |
| OWA-T3 | Open protected email (DNF) in OWA | On a machine that doesn't have the RMS client installed, use a supported browser to connect to OWA in an Exchange 2013/2010 server as the user indicated as a recipient in OWA-T1. Open the protected email and confirm that you can view the email but can't copy, forward or print. If using Exchange Server 2010 SP1 or later, open the attachments in the browser. | User should be able to view the email in the browser. Copy, Print and forward options should not work, (though Print Screen should not be restricted). If using Exchange Server 2010 SP1 or later, attachments should open in the browser and exhibit the same restrictions as the email. |

Table 1: Active Directory Rights Management Services Use Cases

* 1. Before the tests

In order to speed-up the testing process it is recommended that the preparation steps indicated below are performed:

1. A set of generic Office documents need to be created for use during the tests. At least a Word document, an Excel spreadsheet and a PowerPoint presentation should be built, containing some generic text.
2. Templates for testing should be built and deployed to the test clients.
3. If desired, install on the test clients the IRMDiagnosticsTool (as indicated above) to speed-up troubleshooting in case of problems.
4. Copy the list of use cases to an Excel spreadsheet and add columns for Actual Result, Notes and Action Items. Use this spreadsheet to document results of each use case.
   1. Test Methodology

During each functional test, the following steps should be taken for each communication path:

1. Log on to the computers with the appropriate privileges; user accounts used for testing should not have administrative privileges on the client or server systems and should not be members of the SuperUsers group.
2. Depending on the test scenario, there will be different tests to perform. Some tests should be performed under multiple circumstances such as from an intranet-connected computer and an extranet connected computer. You can either multiply the use cases as needed or include the multiple scenarios as variations of the relevant use cases.
3. Validate the test results and document the results in the spreadsheet built in the previous section.
4. Appendix A: Azure Rights Management Services Network Communication Dataflow

This appendix presents the dataflow/communications traffic that may exist within the different scenarios implemented in this solution. The communication process and the TCP/IP ports required for communication between each component shall be included. Currently, collaboration from Azure RMS to AD RMS is not available.

These definitions should be useful for researching communication problems between components if problems arise during testing.

Note: All Azure RMS dataflow in the recommended RMS deployment will take place over 443 TCP. The following information is included as a reference guide for AD RMS dataflow.

* 1. RMS Architecture – Data Flow Required for Base Architecture

This section presents the basic communication requirements between each Azure Rights Management Services component in a base architecture deployment.

The communication requirements assume that each solution component belongs to a different or isolated network.

**Base communication requirements – traffic FROM domain members (RMS Clients, Active Directory Rights Management Services** **Servers, and SQL Servers) TO DCs**

| **Services**  **(Dependencies)** | | **Ports** | | **Notes** |
| --- | --- | --- | --- | --- |
| **OUTBOUND TRAFFIC (TO Domain Controllers only)** | | | | |
| ICMP | ICMP (Ping)  ICMP Code 0  ICMP Type 8 | | ICMP | |
| DNS | 53 UDP/TCP | | Domain Name System Protocol | |
| Kerberos | 88 UDP | | Kerberos V authentication protocol (UDP) | |
| NTP | 123 UDP | | Network Time Protocol (UDP) | |
| Communication to Domain Controllers To Authenticate Users/Groups | 135  (1024-65534 Randomly Allocated High TCP Ports) | | **Remote Procedure Call (RPC) - Endpoint Mapper (All RPC Interfaces)**  ISA 2004 provides a custom RPC filter and makes it easier to use for RPC secondary connections.  In addition, you can restrict   * RPC pool traffic modifying and defining and RPC Range Pool, and create uses that range for that purpose. * RPC UUDIs required to connect to Domain Controllers.   More information:  [How to configure RPC dynamic port allocation to work with firewalls](http://support.microsoft.com/kb/154596/) | |
| Lightweight Directory Access Protocol (LDAP) | 389 UDP/TCP | | Lightweight Directory Access Protocol | |
| Microsoft CIFS (TCP) | 445 TCP | | Microsoft CIFS (TCP) | |
| LDAP (Global Catalog) | 3268 TCP | | Lightweight Directory Access Protocol global catalog protocol | |

Table – Base communication requirements – traffic FROM domain members (RMS Clients, Active Directory Rights Management Services Servers, SQL Servers) TO Domain Controllers

**Communication requirements – FROM Active Directory Rights Management Services cluster TO SQL Server**

|  |  |  |  |
| --- | --- | --- | --- |
| **Services**  **(Dependencies)** | **Ports** | **Notes** | **Services**  **(Dependencies)** |
| **OUTBOUND TRAFFIC (TO Database Server where Active Directory Rights Management Services** **databases reside)** | | | |
| SQL Client Connectivity |  | 1433 TCP | Microsoft SQL Server protocol for connectivity with SQL Server |

Table –Communication requirements – traffic FROM Active Directory Rights Management Services cluster nodes TO SQL Server

**Communication requirements – FROM internal and external Active Directory Rights Management Services client TO Active Directory Rights Management Services cluster**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Services**  **(Dependencies)** | **Ports** | **Notes** | **Services**  **(Dependencies)** | |
| **INBOUND TRAFFIC (Intranet and extranet requests)** | | | |
| Active Directory Rights Management Services Client and Right Management Add-on for Internet Explorer | 443 TCP  -- | | HTTPS/SSL Service  Allow connections from external or internal users to the Active Directory Rights Management Services certification and licensing cluster using only SSL connections (based on this document, scenario can be 80). |

Table –Communication requirements – Traffic FROM Internal and External Active Directory Rights Management Services clients TO Active Directory Rights Management Services Servers

**Communication requirements – additional ports required (Optional)**

| **Services**  **(Dependencies)** | **Ports** | **Notes** |
| --- | --- | --- |
| **OUTBOUND Traffic to Domain Controllers (if required)** | | |
| LDAPS | 636 TCP | Secure Lightweight Directory Access Protocol |
| LDAPS (Global Catalog) | 3269 TCP | Secure Lightweight Directory Access Protocol global catalog protocol |
| **NetBIOS Outbound traffic (if required)** | | |
| NetBIOS Name Service protocol | 137 UDP | NetBIOS Name Service protocol |
| NetBIOS Datagram protocol | 138 UDP | NetBIOS Datagram protocol |
| NetBIOS Session protocol | 139 TCP | NetBIOS Session protocol |

Table –Communication requirements – Additional Ports required (Optional)

* + 1. RMS Architecture – Data Flow Required for Trusted User Domains – Business to Business (B2B)

This scenario presents the dataflow communication requirements for a business to business (B2B) Active Directory Rights Management Services solution.

The communication requirements assume that each solution component belongs to a different or isolated network.

**Base communication data flow**

* Each organization needs to have all connectivity required to access its local Active Directory Rights Management Services domain.

**Additional requirements**

* In addition to accessing local RMS, domain users must also be configured to access the external company Active Directory Rights Management Services domain, which requires the following services.

|  |  |  |  |
| --- | --- | --- | --- |
| **Services**  **(Dependencies)** | **Ports** | **Notes** | |
| **OUTBOUND TRAFFIC (Intranet and Extranet Requests)** | | |
| Rights Management Services Client and Rights Management Add-on for Internet Explorer | 80/443 TCP | HTTPS/SSL Service  Allow connections from external and internal users to the Active Directory Rights Management Services certification or licensing cluster using only SSL connections. |

Table – Data flow required for trusted user domains – business to business (B2B)

**IMPORTANT:** In addition to network access configuration, the clients from each domain require anonymous access to **/\_wmcs/licensing/license.asmx** file.

* + 1. RMS Architecture – Data Flow Required for Trusted User Domains – Intra-organization

This scenario presents the dataflow communication requirements for a trusted user domain deployed in the same organization with more than one forest.

The communication requirements assume that each solution component belongs to a different or isolated network.

**Base communication data flow**

* All clients of each forest need to have all connectivity required to access their local Active Directory Rights Management Services domain.

**Additional requirements**

* For the local Active Directory Rights Management Services users to access the remote company licensing cluster, the Active Directory Rights Management Services domain requires the following services.

|  |  |  |  |
| --- | --- | --- | --- |
| **Services**  **(Dependencies)** | **Ports** | **Notes** | |
| **OUTBOUND TRAFFIC (Intranet and Extranet Requests)** | | |
| RMS Client and Rights Management Add-on for Internet Explorer | 80/443 TCP | HTTPS/SSL Service  Allow connections from external and internal users to the Active Directory Rights Management Services certification or licensing cluster using only SSL connections. |

Table – Data flow required for trusted user domains – internal network – traffic FROM internal clients TO Active Directory Rights Management Services clusters in the internal network

* + 1. RMS Architecture – Data Flow Required for Trusted Publishing Domains – Internal

This scenario presents the dataflow communication requirements for a Trusted Publishing Domain deployed in the same company with more than one forest.

The communication requirements assume that each solution component belongs to a different and isolated network.

**Forest 1 (RMS Domain 1)**

* Same requirements as base scenario for an Active Directory Rights Management Services cluster in its own forest.

**Forest 2 (RMS Domain 2)**

* Same requirements as base scenario for an Active Directory Rights Management Services cluster in its own forest.

**Additional Considerations – Active Directory Rights Management Services clients from both Active Directory Rights Management Services domains accessing licensing cluster**

* Same requirements as base scenario for an Active Directory Rights Management Services cluster in its own forest.

**Additional Considerations – Active Directory Rights Management Services licensing server contacting certification cluster**

* Same requirements as base scenario for an Active Directory Rights Management Services cluster in its own forest.

**Additional Considerations – Active Directory Rights Management Services licensing server contacting SQL Server**

* Same requirements as base scenario for an Active Directory Rights Management Services cluster in its own forest.

**Additional Considerations – Active Directory Rights Management Services group expansion queries lookups**

* Same requirements as base scenario for an Active Directory Rights Management Services cluster in its own forest.

**GAL Synchronization**

* Please check the documentation of the tools in use for GAL synchronization for communications requirements.
  + 1. RMS Architecture – Data Flow Required for Federation Trust – Business to Business

This scenario presents the dataflow communication requirements for a federation trust using Active Directory Federation Services (AD FS) deployed between two organizations.

The communication requirements assume that each solution component belongs to a different/isolated network.

**Base communication data flow**

* All clients in the resource forest need to have all connectivity required to access their local Active Directory Rights Management Services domain.

**Additional requirements**

* For the Active Directory Rights Management Services users in the Accounts forest to access the remote company certification and licensing clusters and the AD FS servers, clients in the Accounts forest require the following services.

|  |  |  |  |
| --- | --- | --- | --- |
| **Services**  **(Dependencies)** | **Ports** | **Notes** | |
| **OUTBOUND TRAFFIC (Intranet and Extranet Requests)** | | |
| Rights Management Services Client | 80/443 TCP | HTTPS/SSL Service  Allow connections to the Active Directory Rights Management Services Certification or Licensing Cluster as well as to the remote Active Directory Federation Services servers using only SSL connections. |

Table – Data flow required for federated trust– traffic FROM clients in the Accounts domain TO Active Directory Rights Management Services clusters in the Resources domain

* For the AD RMS and AD FS servers in the Resources forest to be able to receive requests from the clients in the Accounts forest, they require the following services.

|  |  |  |  |
| --- | --- | --- | --- |
| **Services**  **(Dependencies)** | **Ports** | **Notes** | |
| **INBOUND TRAFFIC (Intranet and Extranet Requests)** | | |
| Rights Management Services | 80/443 TCP | HTTPS/SSL Service  Allow connections from external users to the Active Directory Rights Management Services certification or licensing cluster using only SSL connections. |
| Active Directory Federation Services | 80/443 TCP | HTTPS/SSL Service  Allow connections from external and internal users to the Active Directory Federation Services pipelines using only SSL connections. |

Table – Data flow required for federated trust – traffic TO AD RMS and Active Directory Federation Services in the Resources domain from remote users