Information Rights Management in Office for Mac 2011 Deployment Guide

Table of contents

Overview 1
About this document 1
Setting up IRM for Office for Mac 2
Step 1: Prepare to install the AD RMS role on Windows 7 and Windows Server 2008 R2 SP1 RC or a later version 2
Step 2: Install the AD RMS role on Windows 7 and Windows Server 2008 R2 SP1 RC or a later version 5
Step 3: Configure AD RMS to connect to a Mac computer 7
Step 4: Enable certification of server services 7
Step 5: Verify the AD RMS setup 8
Step 6: Verify the IRM functionality 8
Troubleshooting the setup 10
Providing custom rights management policy templates in Office for Mac 2011 12
Using IRM in Office for Mac 14
Predefined groups of permissions 15

Overview

Information Rights Management (IRM) is an information protection technology that helps protect valuable digital information — such as financial reports, product specifications, customer data, and e-mail messages — from unauthorized users. By using IRM, users can choose from different permission policies to define who can open, change, print, forward, and take other actions with the information. Usage restrictions enforced with IRM are persistent. This means that if a document or e-mail message is using IRM, the permission and usage restrictions are enforced regardless of where the information is moved.

With IRM in Office for Mac, information workers who use Mac computers can receive and consume IRM-enabled documents or e-mail messages. For information technology (IT) managers, IRM helps enforce corporate policies that govern the control and dissemination of confidential information for both Windows and Mac users.

Applying IRM permissions to documents or e-mail messages requires the following:

- Access to Active Directory Rights Management Service (AD RMS) on Windows 7 and Windows Server 2008 R2 Service Pack 1 (SP1) Release Candidate (RC) or a later version to authenticate permissions
- Office for Mac 2011 applications to create IRM permissions

About this document

The Information Rights Management in Office for Mac 2011 deployment guide describes the step-by-step process to set up AD RMS in a test environment, configure this server to work with the Mac clients, and use IRM with Office for Mac.

This document is for IT managers, system administrators, or other people who are responsible for testing IRM implementation in Office for Mac.

Setting up IRM for Office for Mac

This section lists the step-by-step process for installing AD RMS in a test environment and connecting the Mac clients to the AD RMS server for testing the IRM service with Office for Mac 2011.

Note: The step-by-step guide is meant for test environments only. Step-by-step guides are not necessarily meant to be used to deploy Windows Server features without additional deployment documentation and should be used with discretion as a stand-alone document.

Step 1: Prepare to install the AD RMS role in Windows 7 and Windows Server 2008 R2 SP1 RC or a later version

Step 2: Install the AD RMS role in Windows 7 and Windows Server 2008 R2 SP1 RC or a later version

Step 3: Configure AD RMS to connect to a Mac computer

Step 4: Enable certification of server services

Step 5: Verify the AD RMS setup

Step 6: Verify the IRM functionality

Step 1: Prepare to install the AD RMS role on Windows 7 and Windows Server 2008 R2 SP1 RC or a later version

1. Before you install AD RMS on Windows Server 2008 for the first time, make sure that the prescribed requirements are met. To learn more about the requirements, see Pre-installation Information for Active Directory Rights Management Services.

2. The following table lists the system requirements for AD RMS in Windows 7 and Windows Server 2008 R2 SP1 RC or a later version.

Software	Requirement
Operating system	Windows 7 and Windows Server 2008 R2 SP1 RC or a later version Download Windows 7 and Windows Server 2008 R2 Service Pack 1 (SP1) Release Candidate (RC)
Processor	64-bit
File system	NTFS file system is recommended
Web services	Internet Information Services (IIS) ASP.NET must be enabled.
Database server	AD RMS requires a database and stored procedures to perform operations. You can use Microsoft SQL Server 2000 SP3a or a later version, or Microsoft SQL Server 2005. For testing or other single-computer deployment, you can use the Windows internal database on the AD RMS server.
Active Directory directory service	AD RMS must be installed in an Active Directory domain in which the domain controllers are running Windows Server 2008 SP2 or a later version. All users and groups that use AD RMS to consume and publish content must have an e-mail address that is configured in Active Directory. Configurations that use federated services are not supported.
LDAP service	The LDAP service should be installed on the domain controller. This is required for the Autodiscover service. The Autodiscover service automatically discovers the AD RMS server for the client computers.

The following table lists the system requirements for the Mac clients that will be using the IRM feature.

Software	**Requirement**
Processor	Intel only
Operating system	Mac OS X v10.5 (Leopard) or a later version
Memory	1 GB of RAM or more
Hard disk	2.5 GB of available hard disk space HFS +, also known as Mac OS Extended format
Applications	Office for Mac 2011 Volume License copies are required to apply IRM protection to files. Office for Mac Home and Business 2011, Office for Mac Home and Student 2011, and Office for Mac Academic 2011 can only read files protected with IRM. To determine your version, on the application menu, click **About *application***.

Step 2: Install the AD RMS role on Windows 7 and Windows Server 2008 R2 SP1 RC or a later version

1. Install the following roles on Windows 7 and Windows Server 2008 R2 SP1 RC or a later version:
   a. Active Directory Rights Management Services (AD RMS)
   b. Web Server (IIS): Install the Web Server role with the default settings.
2. Choose a database that AD RMS can use to store configuration and policy information. The database can be hosted either by Windows Internal Database or another database server.

   Note: Using Windows Internal Database will limit this AD RMS cluster to a single-server cluster. If you intend to join more servers to the AD RMS cluster, use a SQL server.
3. Select a domain user account that is required to provide a network identity for AD RMS so that it can communicate with servers on the network.
4. For the test scenario, create a self-signed certificate for Secure Sockets Layer (SSL) encryption.

Setting up AD RMS and Web Server roles on the test server

1. Click **Start**, point to **Administrative Tools**, and then click **Server Manager**.
2. On the **Before You Begin** page, read and verify the instructions, and then click **Next**.
3. On the **Select Server Roles** page, select the **Active Directory Rights Management Services** and the **Web Server (IIS)** check boxes, and then click **Next**.
4. Read the **Active Directory Rights Management Services** page, and then click **Next**.
5. In the **Role services** box, make sure that **Active Directory Rights Management Server** is selected, and then click **Next**.
6. Click the **Create a new AD RMS cluster** option, and then click **Next**.
7. Click the **Use Windows Internal Database on this server** option, and then click **Next**.
8. Click **Specify**, type **<*domain\username*>**, type the password for the account, click **OK**, and then click **Next**.

   Note: This domain user account should differ from the account that is used to log on to the server. This should not be a domain administrator account.
9. Click the **Use AD RMS centrally managed key storage** option, and then click **Next**.

10. Type a strong password in the **Password** box and in the **Confirm Password** box, and then click **Next**.
11. Choose the Web site where AD RMS will be installed, and then click **Next**.

    Note: If you are using Secure Sockets Layer (SSL), then select an HTTP site with SSL. If you are not using SSL, then select an HTTP site. Windows Authentication is a required authentication option on a non-SSL site.
12. Click the **Use an SSL-encrypted connection (https://)** option.

    Note: We recommend that you use an SSL connection.
13. In the **Fully-Qualified Domain Name** box, type ***%servername%.*<domainname>.com**, and then click **Validate**.

    If validation succeeds, the **Next** button becomes available. Click **Next**.

    Note: 443 is the default port for HTTP with SSL.
14. If the SSL site doesn't have a server authentication certificate, click **Create a self-signed certificate for SSL encryption**.

    Note: The self-signed certificate is only required if the SSL site does not have a Server Authentication certificate. If the SSL site has a Server Authentication certificate, then select the certificate later.
15. Select the **Register the AD RMS service connection point later** option, and then click **Next**.

    Note: The service connection point (SCP) for AD RMS identifies the connection URL for the service to the AD RMS-enabled clients in your organization. After you register the SCP in Active Directory Domain Services (AD DS), clients will be able to discover the AD RMS cluster to request use licenses, publishing licenses, or rights account certificates (RACs). There can only be one discoverable RMS server on a domain, so select the **Register the AD RMS service connection point later** option only if you are using a test server in a production domain. If the test server is located on a domain where you want to make it discoverable, then you must register the service connection point by selecting the **Register the AD RMS service connection point now** option.
16. Click **Next** to install the Web Server role.
17. Keep the default role Web services, and then click **Next**.
18. Click **Install**.
19. Click **Close**.

    After the installation, log off and log on for the changes to take effect.

Step 3: Configure AD RMS to connect to a Mac computer

You must upgrade the AD RMS service to configure it to work with Mac computers.

Open Windows Explorer and browse to the System 32 folder.

By default, the folder path is **%systemdrive%\Windows\System 32**.

1. In the System 32 folder, double-click **regedt32**.
2. Under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DRMS, double-click **ConfigStatus**.
3. In the **Edit DWORD (32-bit) Value** box, change the **Value Data** to **2**, and then click **OK**.

   In Windows Explorer, browse to the **RMS** folder.
4. By default, the folder path is **%systemdrive%\Windows\System 32\rms**.
5. In the rms folder, right-click **Microsoft.RightsManagementServices.UpgradeWizard**, and then click **Run as administrator**.
6. On the **Active Directory Rights Management Services** page, click **Next**.
7. On the **Provide AD RMS Service Account Password** page, enter the same password that was used in the RMS installation.
8. On the **Provide AD RMS Private Key Password** page, enter the same password that was used to encrypt the private key in the RMS installation.
9. On the **Confirm Installation Options** page, click **Install**.
10. Click **Close**.

Step 4: Enable certification of server services

Open Windows Explorer and browse to the folder where IIS is installed.

By default, the folder path is **%systemdrive%\inetpub\wwwroot_wmcs\certification**.

1. To enable server services to receive RACs, right-click the **MacCertification.asmx** file, and then click **Properties**.
2. On the **Security** tab, and click **Continue**.
3. On the **Security** tab, click **Add**.

   Verify the permitted users on the **Security** tab. You should see System, AD RMS Service Group, Administrators, and Users. If these accounts objects are missing from the Security tab, then go to step 4 to add them.
4. To add the computer account object of the AD RMS-enabled server application and the AD RMS Service Group, click **Locations**.

5. Select ***%servername%***, and then click **OK**.
6. Click **Advanced**.
7. Click **Find Now**.
8. Select the following groups from the search results:
    - AD RMS Service Group (%servername% \AD RMS Group)
    - Administrators (%servername% \Administrators)
    - Users (%servername% \Users)
9. Click **OK**.

Step 5: Verify the AD RMS setup

After you set up AD RMS, you can verify the setup by testing the server licensor certificate (SLC). The SLC is created when the AD RMS server role is installed and configured on the first server in the cluster.

1. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Rights Management Services**.
2. On the **Cluster Details** group box, under **Intranet cluster URL**s, click the **Certification URL**.

    You should see the **CertificationWebService** page with a **Certify** link on it.

To verify that a client computer can connect to the AD RMS server, use the client to browse to the following link:

http://<*fully.qualified.domain.name*>/_wmcs/certification/certification.asmx

where the fully-qualified domain name is the AD RMS server. You should see the **CertificationWebService** page.

Step 6: Verify the IRM functionality

On a Windows client, restrict permissions for an Outlook (for Windows) e-mail message and send it to the Mac users who will be using IRM in Office for Mac.

Note: If the AD RMS server that you configure is the primary AD RMS server on the domain, then the Windows and Mac clients in that domain will connect to the server automatically by using the Autodiscovery service. However, if you are working in a test environment and the AD RMS server is not the primary server, you must first configure a Windows client to connect to the AD RMS server. Then you create the e-mail message and send it to the Mac clients. See Configure an Office (for Windows) client to connect to the AD RMS in the test environment.

Configure an Office (for Windows) client to connect to the AD RMS in the test environment

Important:

Perform the following step only if the AD RMS server that you set up is not the primary AD RMS server in the domain.

To configure the Windows client, follow these steps:

1. Delete the Digital Rights Management (DRM) store from %localappdata%\Microsoft\DRM.
2. If you used IRM with Office 2007 (for Windows), delete any registry keys from these locations:
   - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Office\12.0\Common\DRM
   - HKEY_LOCAL_MACHINE\SOFTWARE \Microsoft\Office\12.0\Common\DRM
3. When you open an AD RMS-enabled application, the application retrieves the rights policy templates from the assigned path, which is specified in a registry location. This location can vary, depending on the application. Configure the new server information in the registry keys listed here:

Processor	Registry key path	New value
32-bit	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSDRM\ServiceLocation\Activation	Type: REG_SZ (String Value) Value= https://<servername>.<fully_qualified_domainname>.com:443/_wmcs/certification
64-bit	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MSDRM\ServiceLocation\Activation	Type: REG_SZ (String Value) Value=https://<servername>.<fully_qualified_domainname>.com:443 /_wmcs/certification

Troubleshooting the setup

Issue

In a production environment, Office tries to connect to the primary AD RMS server in the domain instead of your test server even after you modify the registry keys and delete the DRM folder.

Solution

1. Delete any DRM-related registry keys from the following locations:
   - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Office\12.0\Common\DRM
   - HKEY_LOCAL_MACHINE\SOFTWARE \Microsoft\Office\12.0\Common\DRM
   - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\12.0\Common\DRM
2. Office may be looking for the registry keys in a different location. Try entering the following keys:

Processor	Registry key path	New value
32-bit	HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\Office\12.0\Common\DRM	• name = CorpCertificationServer, type = REG_SZ (String Value), value = https://<servername>.<fully_qualified_domainname>.com:443 /_wmcs/certification • name = CorpLicensingServer, type = REG_SZ (String Value), value = Value=https://<servername>.<fully_qualified_domainname>.com:443 /_wmcs/licensing
64-bit	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Office\12.0\Common\DRM	• name = CorpCertificationServer, type = REG_SZ (String Value), value = https://<servername>.<fully_qualified_domainname>.com:443 /_wmcs/certification • name = CorpLicensingServer, type = REG_SZ (String Value), value = Value=https://<servername>.<fully_qualified_domainname>.com:443 /_wmcs/licensing

Issue

After migrating data with the Data Migration wizard on a Mac client, IRM no longer works.

Solution

1. Delete the following folder: ~/Library/Application Support/Microsoft/Office/DRM
2. Delete the following files:
   - ~/Library/Preferences/ByHost/MicrosoftRegistrationDB*.plist
   - ~/Library/Preferences/com.microsoft.MicrosoftOfficeDRM.plist
3. Open the **Keychain Access** application, and remove the following **login** keychains:
   - corprights*
   - com.microsoft.ipc.h
   - com.microsoft.ipc.k

If IRM still does not work, check the configuration of the AD RMS server.

Issue

IRM does not work on a Mac client.

Solution

1. Verify that IRM is turned on.
2. Verify that the client has the correct network settings, including search domain.
3. Ensure that the server is set up for Mac clients (see Step 3: Configure AD RMS to connect to a Mac computer in this document).

Providing custom rights management policy templates in Office for Mac 2011

A rights policy template that is stored in the AD RMS server defines the rules and conditions for using content. Templates can include various rules, such as which users and groups have rights to work with the content that is protected, permission levels, and the date that the content expires on. As an administrator, you can create customized permission policies for the users in your organization by creating the rights policy templates. You manage the rights policy templates from the AD RMS Administration site on the Windows RMS server. When you create the rights policy template on the RMS server, the Mac clients can automatically apply the rules that are defined in the template.

Note: For AD RMS running on Windows 7 and Windows Server 2008 R2 SP1 RC or a later version, rights policy templates are automatically managed by the AD RMS client. A template distribution pipeline enables the AD RMS client to poll for updates to the rights policy templates. If a rights policy template is added, changed, or deleted, the client detects these changes and updates the local rights policy templates during its next refresh.

When you create a new rights policy template, the **Create Distributed Rights Policy Template** or **Create Archived Rights Policy Template** wizard steps you through the different elements of the template, depending on the kind of template that you want. These elements can be modified later by selecting the template and opening its properties sheet.

For more information about how to create a new rights policy template, see Create a New Rights Policy Template on the Microsoft Web site.

The following table lists the IRM permissions right in the rights policy template. Each right can be enforced by Office for Mac 2011 applications that are configured on a network that includes a server that runs AD RMS.

IRM right	Description
Full Control	The user has all the rights listed in this table. Expiration does not apply to users who have Full Control.
View	The user can open the IRM-protected content to view it.
Edit	The user can open, view, and edit the IRM-protected content.
Save	The user can save the IRM-protected content.
Export (Save as)	The user can save the IRM-protected content to another location or format that might support IRM.
Print	The user can print the content.
Forward	The user can forward an IRM-protected e-mail message to another recipient.
Reply	The user can reply to an IRM-protected e-mail message.
Reply All	The e-mail recipients of an IRM-protected message can reply to all users on the To: and Cc: lines.
Extract	The user can make a copy of any part of a file and paste that part into the work area of another application.
Allow Macros	The user can run macros against the contents of a file.
View Rights	The user can view the rights that are associated with a file.
Edit Rights	The user can edit the rights that are associated with a file.

Using IRM in Office for Mac

Here is a typical user workflow for IRM-protected documents:

1. An author creates content in one of the Office for Mac applications — Word, Excel, PowerPoint, or Outlook.
2. The author clicks the **Permission** command on the **Review** tab and enters the names of the individuals or groups that can access the document.
3. The author defines the permission levels for the recipients of the document, such as View, Edit, or Print. In the background, the application communicates with the AD RMS server to apply rights to the file. For more information about how permissions are set in each application, see the Help for the relevant application.
4. After applying permissions, the author distributes the file by using any method, including attaching the file to an e-mail message, posting it to a shared folder, or distributing it on a disk. Because IRM protection is at the file level and is persistent, the usage restrictions move with the document.
5. When the recipient receives the IRM-protected file and opens it, the application communicates with the AD RMS server to determine whether the recipient is an authorized user and has the rights to access the file. AD RMS validates the user and issues a use license. The application renders the file and enforces the rights.

Predefined groups of permissions

Office 2011 provides the following predefined groups of rights that users can choose from when they create IRM content. The options are available in Word 2011, Excel 2011, and PowerPoint 2011. In the Office for Mac application, on the **File** menu, point to **Restrict Permissions**, and then click **Restricted Access** to enable the permission options that are listed in the following table.

IRM predefined group	Description
Read	Users who have Read permissions only have the View right.
Change	Users who have Change permissions have View, Edit, and Save rights.
Full Control	Users with Full Control permissions have every right listed in this table, as well as the right to make changes to permissions associated with content. Expiration does not apply to users who have Full Control.

Users can also specify more advanced IRM permissions in Word 2011, Excel 2011, and PowerPoint 2011. In the **Permission** dialog box, click **More Options**. For example, users can specify an expiration date, let other users print or copy content, and so on.

In Outlook 2011, users can select the following predefined group of rights when they create an e-mail item. Open a new e-mail message, and then on the **Options** tab, under **Permissions**, click **Do Not Forward**.

IRM predefined group	Description
Do Not Forward	In Outlook, the author of an IRM e-mail message can apply the Do Not Forward permission to users on the To, Cc, and Bcc lines. This permission includes the View, Edit, Reply, and Reply All rights.