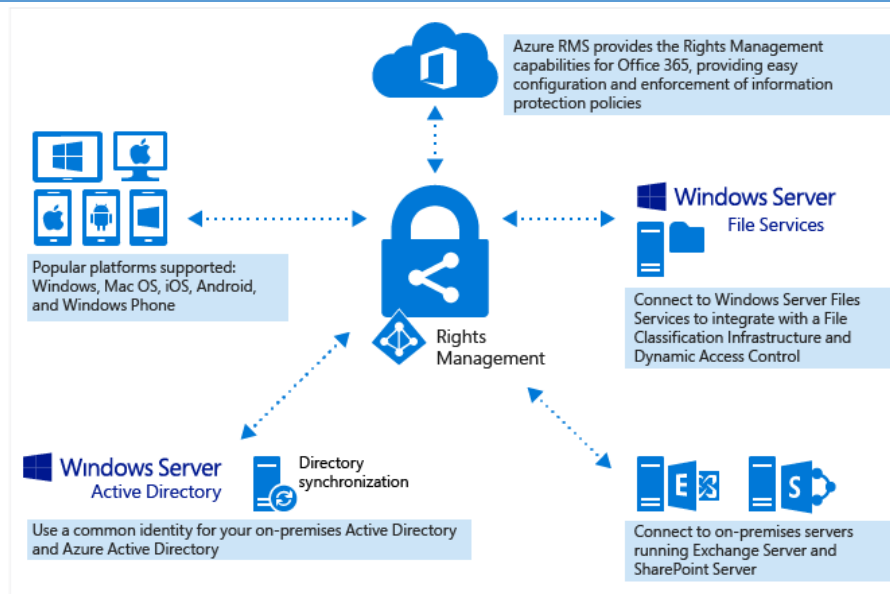


Introduction About Azure RMS



Azure Rights Management (Azure RMS) is an information protection solution for organizations that want to protect their data in today's challenging working environment.

These challenges include the need to be Internet-connected, with users bringing personal device to work, accessing company data on the road and home, and sharing sensitive information with important business partners. As part of their daily work, users share information by using email, file-sharing sites, and cloud services. In these scenarios, traditional security controls (such as access control lists and NTFS permissions) and firewalls have limited effectiveness if you want to protect your company data while still empowering your users to work efficiently.

In comparison, Azure RMS can protect your company's sensitive information in all these scenarios. It uses encryption, identity, and authorization policies to help secure your files and email, and it works across multiple devices—phones, tablets, and PCs. Information can be protected both within your organization and outside your organization because that protection remains with the data, even when it leaves your organization's boundaries. As an example, employees might email a document to a partner company, or they save a document to their cloud drive. The persistent protection that Azure RMS provides not only helps to secure your company data, but might also be legally mandated for compliance, legal discovery requirements, or simply good information management practices.

But very importantly, authorized people and services (such as search and indexing) can continue to read and inspect the data that Azure RMS protects, which is not easily accomplished with other information protection solutions that use peer-to-peer encryption. This ability is sometimes referred to as "reasoning over data" and is a crucial element in maintaining control of your organization's data.

The following picture shows how Azure RMS works as a Rights Management solution for Office 365 as well as for on-premises servers and services. You'll also see that it supports the popular end user devices that run Windows, Mac OS, iOS, Android, and Windows Phone.

Azure RMS Prerequisites

Requirement	More information
A cloud subscription for RMS	<p>Your organization must have a cloud subscription that supports RMS.</p> <p>For licensing information, see the Cloud subscriptions that support Azure RMS section in this topic.</p>
Azure AD directory	<p>Your organization must have an Azure AD directory to support user authentication for RMS. In addition, if you want to use your user accounts from your on-premises directory (AD DS), you must also configure directory integration.</p> <p>Multi-factor authentication (MFA) is supported with Azure RMS when you have the required client software and correctly configured MFA supporting infrastructure.</p> <p>For more information, see the Azure AD directory section in this topic.</p>
Client devices	<p>Users must have a client devices (computer or mobile device) that run an operating system that supports RMS.</p> <p>For more information, see the Client devices that support Azure RMS section in this topic.</p>
Applications	<p>Users must run applications that support RMS.</p> <p>For more information, see the Applications that support Azure RMS section in this topic.</p>
Infrastructure that supports connectivity to the Internet and dependent cloud services	<p>If you have a firewall or similar intervening network devices that must be configured to allow specific connections, see Office 365 URLs and IP address ranges.</p> <p>The list of URLs and IP addresses in the Office 365 portal and identity section apply to the Office 365 portal, Azure Active Directory resources, and Azure Rights Management. Use the instructions in this article to keep up-to-date with changes to this information, by subscribing to an RSS feed.</p> <p>In addition to the information in the Office article, specific to Azure RMS:</p> <p>Do not terminate the TLS client-to-service connection (for example, to do packet-level inspection). Doing so breaks the certificate pinning that RMS clients use with Microsoft-managed CAs to help secure their communication with Azure RMS.</p>

Do not use a web proxy configuration that authenticates on behalf of a user.

What problems does Azure RMS solve?

Requirement or problem	Solved by Azure RMS
Protect all file types	✓ In previous implementation of Rights Management, only Office files could be protected, using native protection. Now, generic protection means that all file types are supported.
Protect files anywhere	✓ When a file is saved to a location (protect in-place), the protection stays with the file, even if it is copied to storage that is not under the control of IT, such as a cloud storage service.
Share files securely by email	✓ When a file is shared by email (share protected), the file is protected as an attachment to an email message, with instructions how to open the protected attachment. The email text is not encrypted, so the recipient can always read these instructions. However, because the attached document is protected, only authorized users will be able to open it, even if the email or document is forwarded to other people.
Auditing and monitoring	<p>✓ You can audit and monitor usage of your protected files, even after these files leave your organization's boundaries.</p> <p>For example, you work for Contoso, Ltd. You are working on a joint project with 3 people from Fabrikam, Inc. You email these 3 people a document that you protect and restrict to read-only. Azure RMS auditing can provide the following information:</p> <ul style="list-style-type: none">• Whether the people you specified in Fabrikam opened the document, and when.• Whether other people that you didn't specify attempted (and failed) to open the document—perhaps because it was forwarded or saved to a shared location that others could access.• Whether any of the specified people tried (and failed) to print or change the document.
Support for all commonly used devices, not just Windows computers	✓ Supported devices include: <ul style="list-style-type: none">• Windows computers and phones• Mac computers• iOS tablets and phones• Android tablets and phones

Support for business-to-business collaboration	<p>✓ Because Azure RMS is a cloud service, there's no need to explicitly configure trusts with other organizations before you can share protected content with them. If they already have an Office 365 or an Azure AD directory, collaboration across organizations is automatically supported. If they do not, users can sign up for the free RMS for individuals subscription.</p>
Support for on-premises services, as well as Office 365	<p>✓ In addition to working seamlessly with Office 365, you can also use Azure RMS with the following on-premises services when you deploy the RMS connector:</p> <ul style="list-style-type: none"> • Exchange Server • SharePoint Server • Windows Server running File Classification Infrastructure
Easy activation	<p>✓ Activating the Rights Management service for users requires just a couple of clicks in the Azure classic portal.</p>
Ability to scale across your organization, as needed	<p>✓ Because Azure RMS runs as a cloud service with the Azure elasticity to scale up and out, you don't have to provision or deploy additional on-premises servers.</p>
Ability to create simple and flexible policies	<p>✓ Customized rights policy templates provide a quick and easy solution for administrators to apply policies, and for users to apply the correct level of protection for each document and restrict access to people inside your organization.</p> <p>For example, for a company-wide strategy paper to be shared with all employees, you could apply a read-only policy to all internal employees. Then, for a more sensitive document, such as a financial report, you could restrict access to executives only.</p>
Broad application support	<p>✓ Azure RMS has tight integration with Microsoft Office applications and services, and extends support for other applications by using the RMS sharing application.</p> <p>✓ The Microsoft Rights Management SDK provides your internal developers and software vendors with APIs to write custom applications that support Azure RMS. For more information, see How Applications Support Azure Rights Management.</p>
IT must maintain control of data	<p>✓ Organizations can choose to manage their own tenant key and use the "Bring Your Own Key" (BYOK) solution and store their tenant key in Hardware Security Modules (HSMs).</p> <p>✓ Support for auditing and usage logging so that you can analyze for business insights, monitor for abuse, and (if you have an information leak) perform forensic analysis.</p> <p>✓ Delegated access by using the super user feature ensures that IT can always access protected content, even if a document was protected by an employee who then leaves the organization. In comparison, peer-to-peer encryption solutions risk losing access to company data.</p> <p>✓ Synchronize just the directory attributes that Azure RMS needs to support a common identity for your on-premises Active Directory accounts, by using a directory synchronization tool, such as Azure AD Connect.</p>

✓ Enable single-sign on without replicating passwords to the cloud, by using AD FS.

✓ Organizations always have the choice to stop using Azure RMS without losing access to content that was previously protected by Azure RMS. For information about decommissioning options, see [Decommissioning and Deactivating Azure Rights Management](#). In addition, organizations who have deployed Active Directory Rights Management Services (AD RMS) can [migrate to Azure RMS](#) without losing access to data that was previously protected by AD RMS.

MAQOOV.org

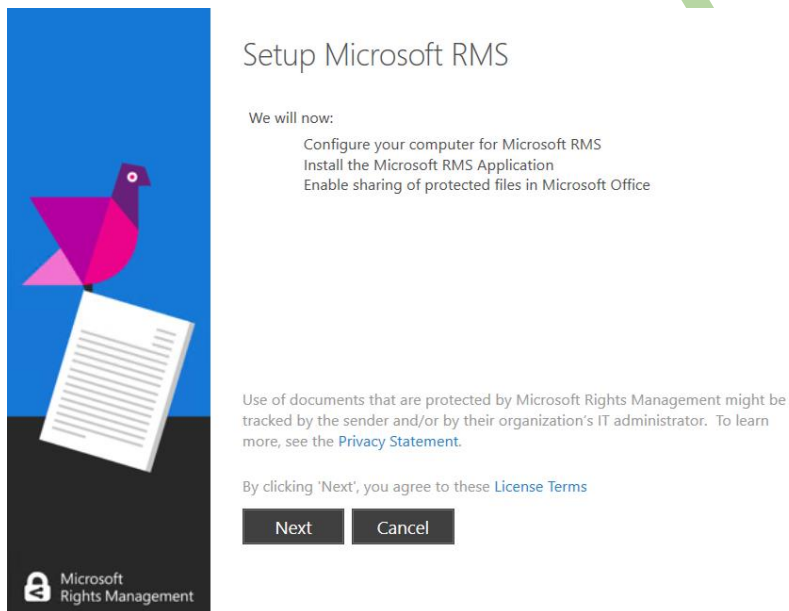
LAB Scenario

In this lab we will start using Azure RMS in our Test Environment to do the following scenarios:

1. Install Azure RMS Sharing application.
2. How to create custom template?
3. Protect document in place between two users.
4. Send protected email.
5. Track Documents.

Azure RMS Guide

1. Download and install Azure RMS From <https://www.microsoft.com/en-gb/download/details.aspx?id=40857>
2. On **Setup Microsoft RMS**, Click **Next**.



3. After the installation is finished close all your apps and save your document and then click restart.



Setting up Microsoft RMS

Configure your computer for Microsoft RMS

Success

Install the Microsoft RMS Application

Success

Enable sharing of protected files in Microsoft Office

Success

To complete installation, you must restart your computer

Close

Restart

Microsoft
Rights Management

How to create custom template?

1. Login to Azure Portal.
2. Select Active Directory.
3. Select Rights Managements Tab, Select **Templates**, Click **ADD** button from down panel.
4. On Add a new rights Policy template
 - a. **Language:** English
 - b. **Name:** Custom_1
 - c. **Description:** Custom_1

Add a new rights policy template

Language

English - United States



Name

Custom_1

Description

Custom_1



5. Click the **Tick** Button.
6. After the template is created select the template and click the arrow button.

Microsoft Azure

Check out the new portal

CREATE STATUS

admin@MAQOV.onmicrosoft.com

MAQOV

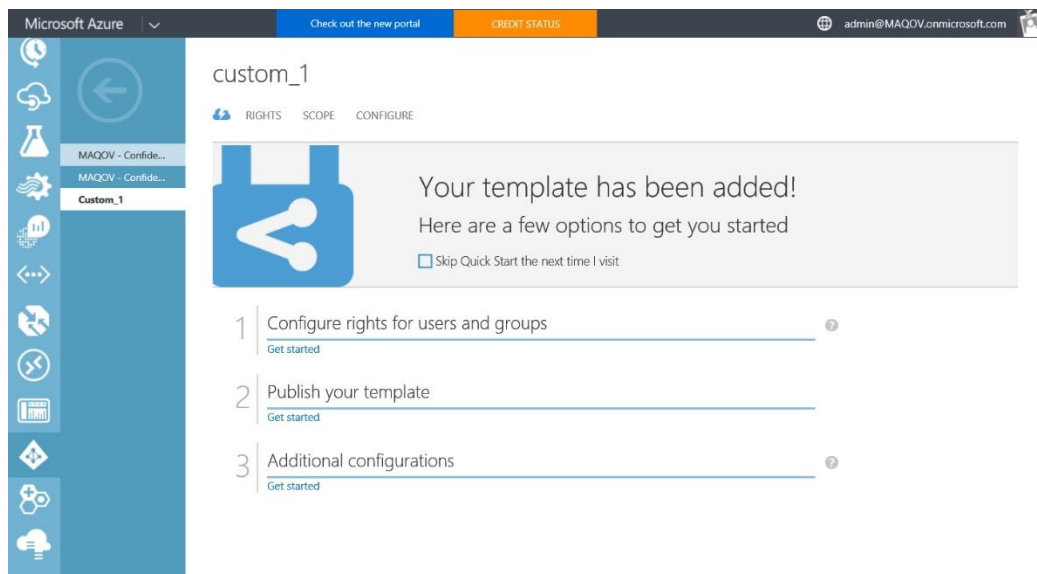
maqov

TEMPLATES

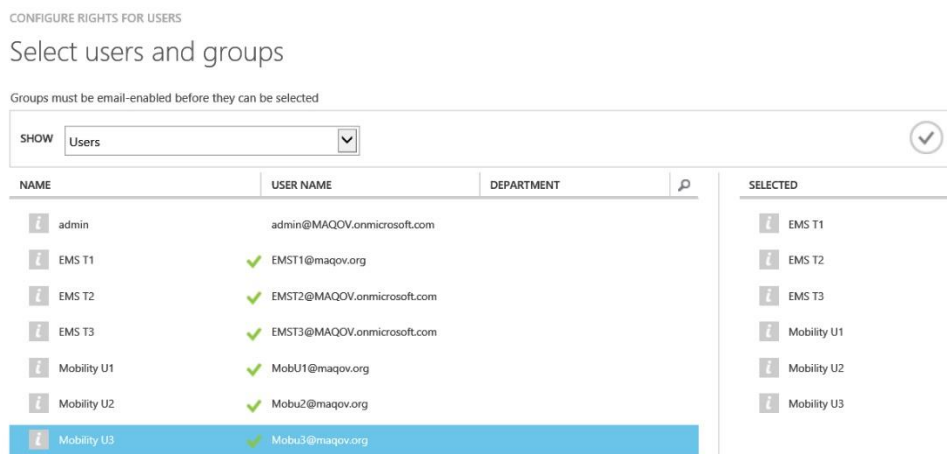
NAME	DESCRIPTION	DATE MODIFIED	STATUS
MAQOV - Confidential	This content is proprietary information int...	2/3/2016 9:59:00 PM	Published
MAQOV - Confidential View Only	This content is proprietary information int...	2/3/2016 9:59:00 PM	Published
Custom_1	Custom_1	2/11/2016 12:55:00 PM	Archived

MAQOV.org

7. Click **Configure rights for users and groups**.



8. Add the desired users, and then click the tick button.



9. On **Assign Custom Rights**, select **Edit Content**, and then Click **Tick** Button.



10. On the **configure** tab, fill the below data.

a. At **general** select **Publish**, in order to make the template appear on the end user side at the sharing application.

b. At the **Content Expiration**, click **Content never expires**

Note You can either make the expiration date valid until specific period in this case you will select **Content Expiration(date)**. or make the validation period expire after specific number of days.

c. On **offline access** select **number of days the content is available without internet access**.

custom_1

RIGHTS SCOPE CONFIGURE

general

STATUS **PUBLISH** ARCHIVE

name and description

LANGUAGE	NAME	DESCRIPTION
English - United States	Custom_1	Custom_1
Select language	NAME	DESCRIPTION

content expiration

☒ Content never expires

☐ Content expiration (date) 2016-05-11

☐ After the content is protected, content expires after the specified number of days

name and description

LANGUAGE	NAME	DESCRIPTION
English - United States	Custom_1	Custom_1
Select language	NAME	DESCRIPTION

content expiration

☒ Content never expires

☐ Content expiration (date) 2016-05-11

☐ After the content is protected, content expires after the specified number of days

offline access

☐ Content is available only with an Internet connection

☐ Content is always available

☒ Number of days the content is available without an Internet connection 7

11. .

12. .

13. .

14. .

15. .

16. .

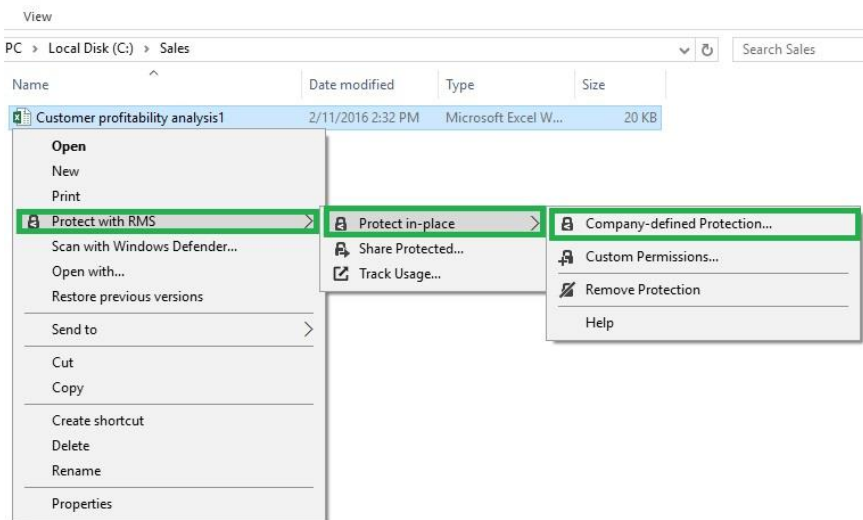
17. ..

18. ..

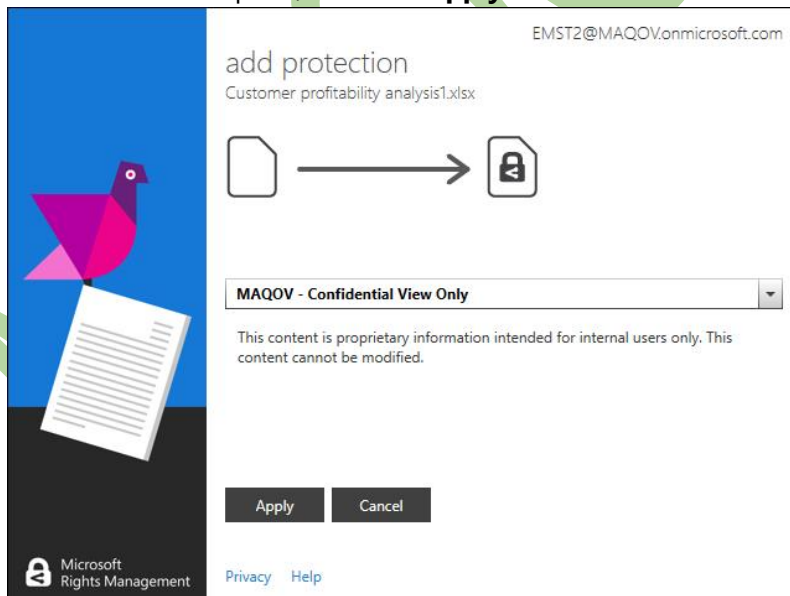
How to Protect Document using Azure RMS Sharing Application in place

In this section the **EMST2** is the user who will protect the document, and **EMST3** is the user who will check the applied permission.

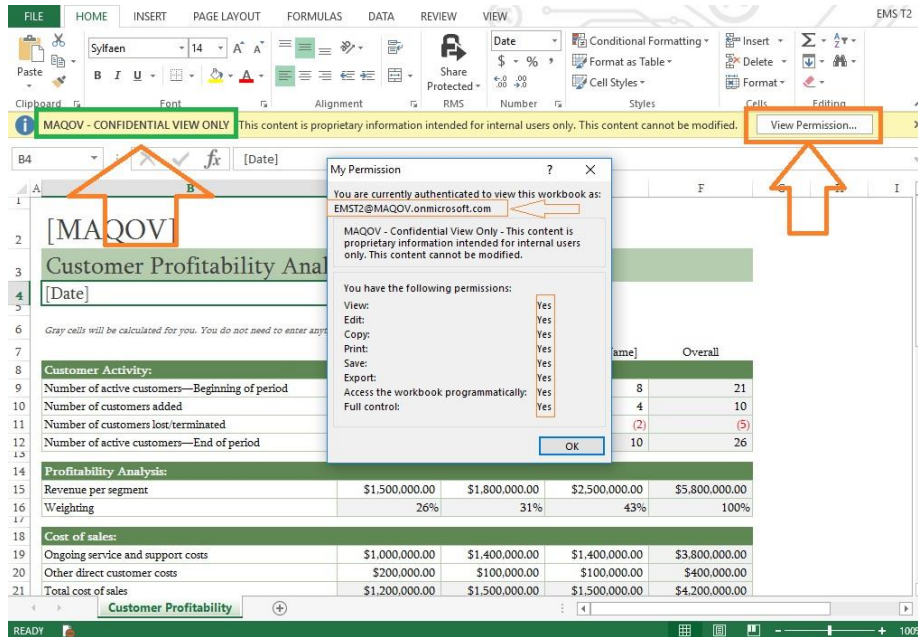
1. Login to the client machine where we installed the Azure RMS Sharing Application.
2. Select the document you need to protect locally.
3. Right click on the document, select **Protect with RMS, Protect in-place, Company-Defined Protection**



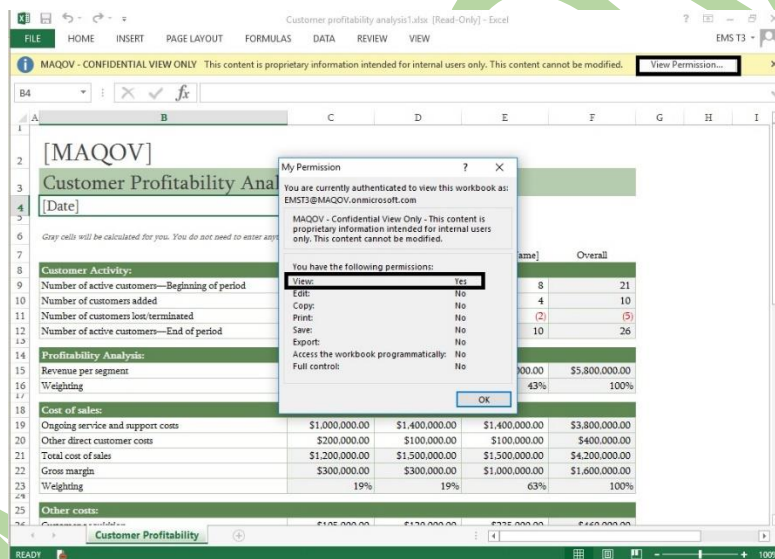
4. Select desired template, and click **Apply**.



5. Open the document after protection to check the permission as the owner you will find that EMST2 has full control.

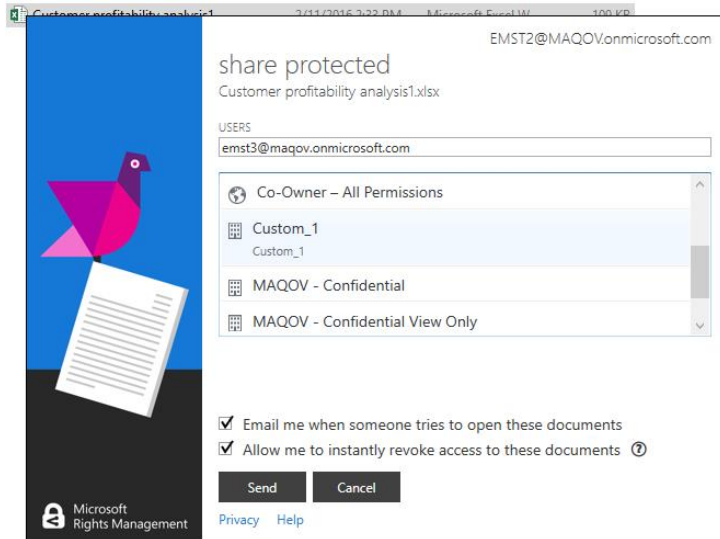


6. Sign-out from the machine and login to the machine using EMST3, to check the permission.
7. You will find that user has View only, this mean that the template is applied successfully.

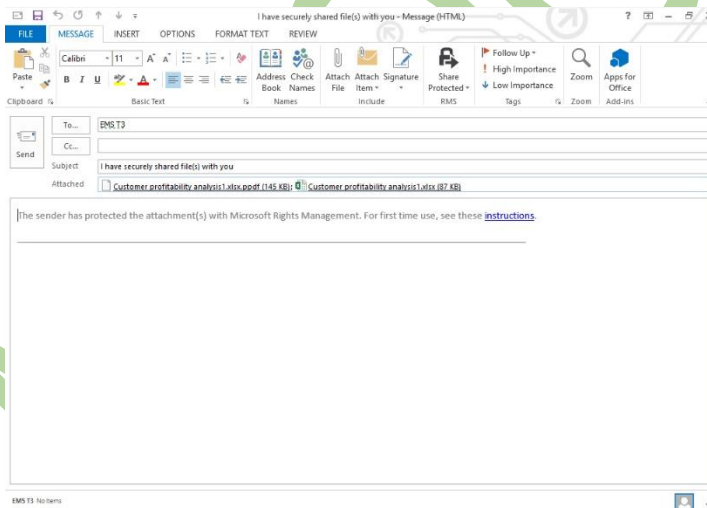


How share protected document using email

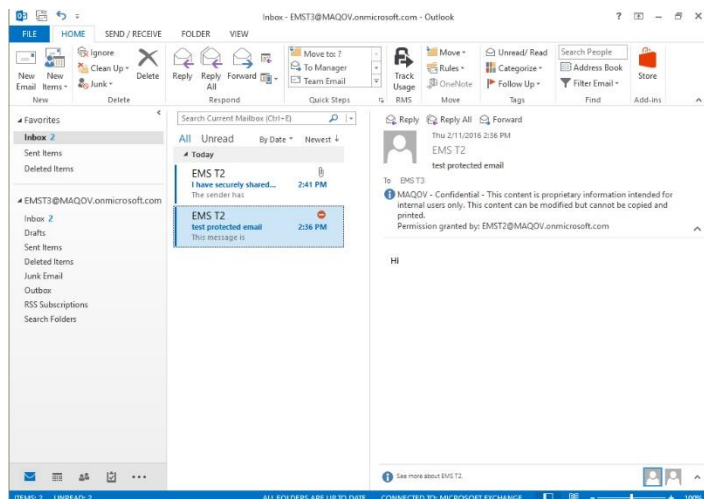
1. Login by **EMST2** to the machine where the Azure RMS Sharing Application is installed.
2. Select the desired file and **right click, protect with RMS**, and **share protected**.
3. In the Users: Write EMST3 EMAIL, Select the Permission, I will select the custom template I created before" Custom_1".
4. Check "**Email Me when someone tried to opens this documents**".
5. Check "**Allow me to instantly revoke access to this documents**".



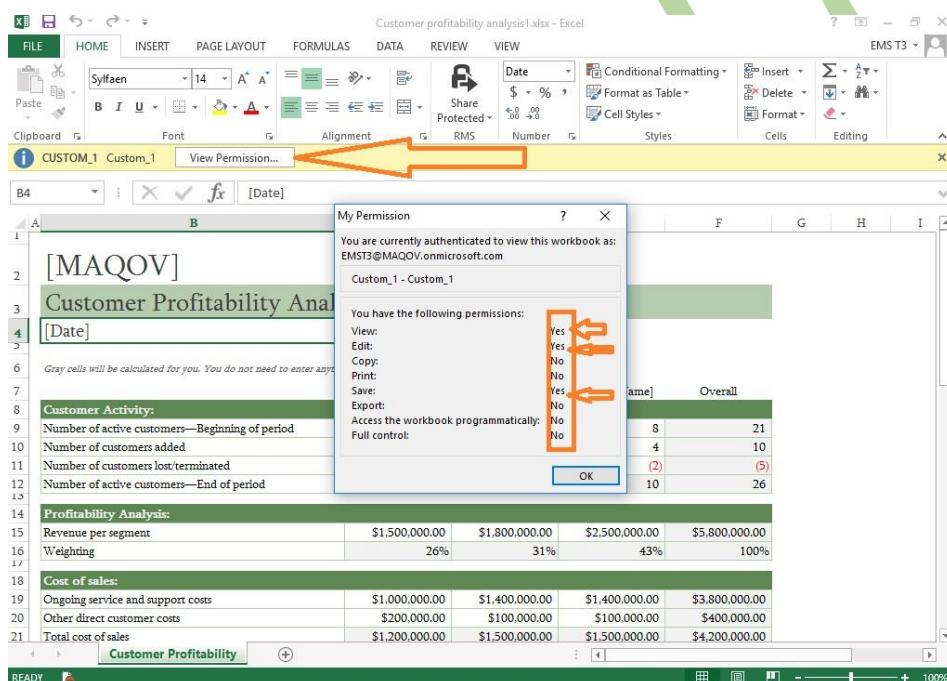
6. Click **Send, automatically outlook will be opened**, click **Send**.
Note you will find to files in the attachment the protected document, and a protected PDF File.
On the [Instructions](#) link this will guide the external users to Sign up for [RMS for individuals](#) in order to be view the document.



7. On EMST3 Outlook he/she will receive an email, open it and download the attachment locally.



8. Check the permission we will find that the custom permission is applied.



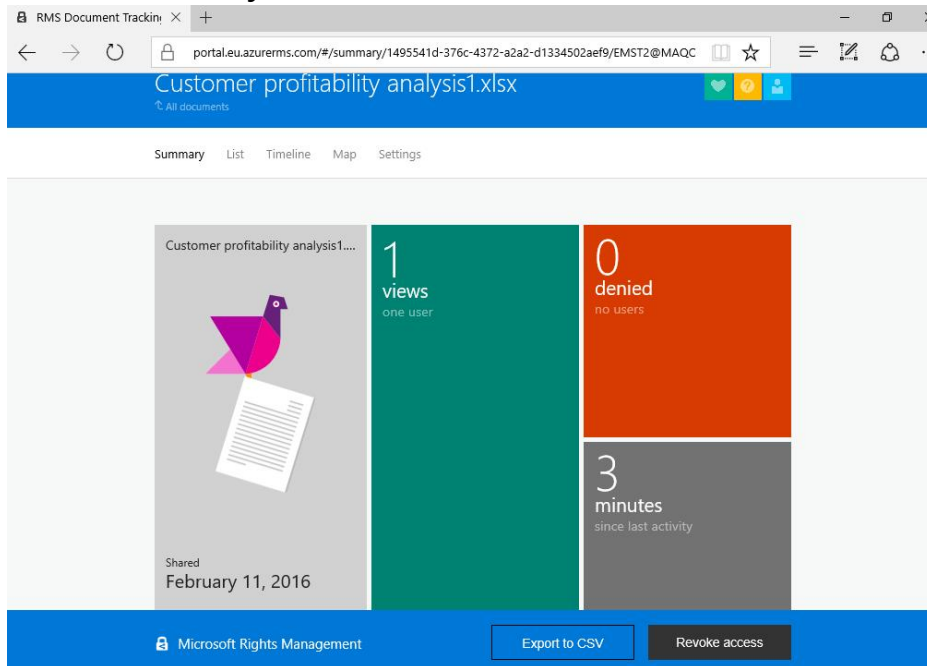
How to send protected email?

In my previous blogpost we described two things how enable IRM with exchange online, or how to send protected email.

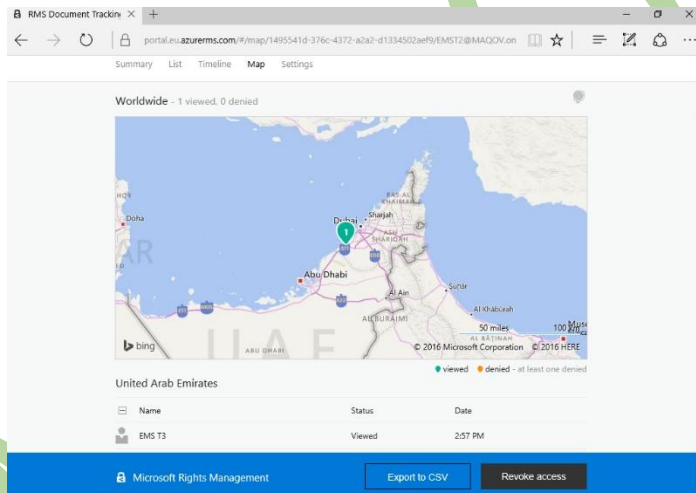
RMS Document Tracking

In this section we will discover the features of Azure RMS Document Tracking Portal

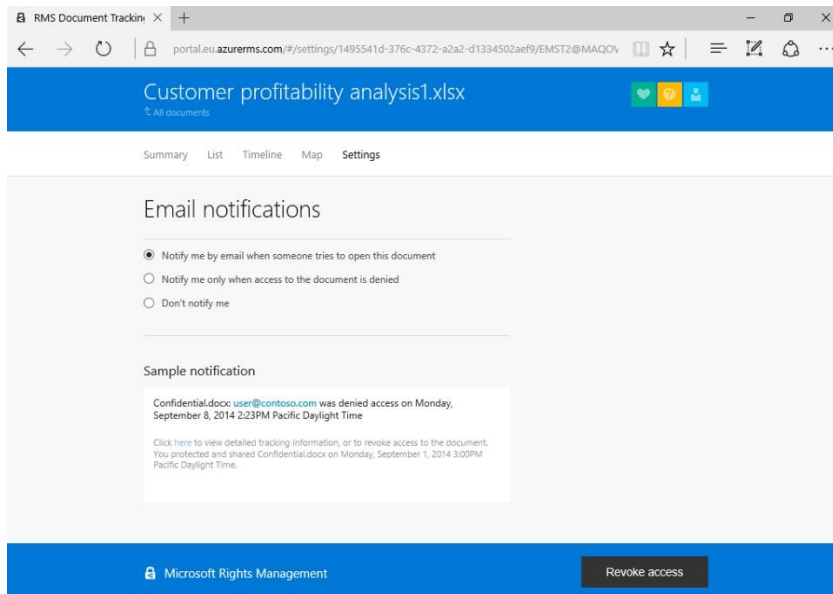
1. Open <https://portal.azureirms.com/> , sign in using **EMST2** Credentials.
2. Check the **Summary Tab**.



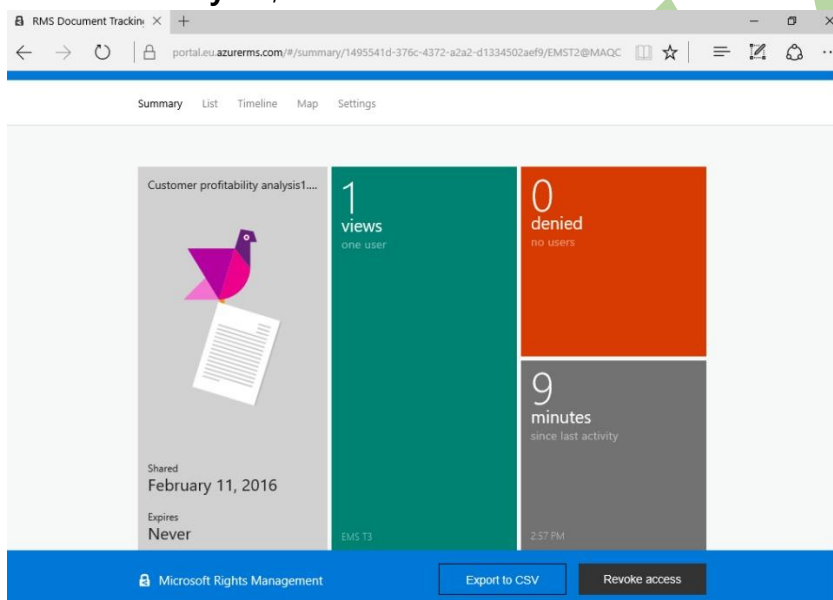
3. Click on the **MAPS** to see check where the document is opened.



4. On the **settings** tab, you can edit the notification settings.



5. On **list** you will find who opened the document and the status it could be **Viewed** or **denied**.
6. On the **Summary** tab, select the document and click **revoke access**.



7. Click **confirm** to complete the revoke process.

